Strategic Trade Review

Spring 2017

Illicit Nuclear Procurement Networks
A Resilience Framework

Chemical and Biological Contract Manufacturing Services
Proliferation Concerns and Impacts

Dual-Use Research and Strategic Trade Controls
Evaluating Trade Controls as a Governance Instrument

Export Control Compliance and Academia
Implications for American Universities

Cyber-Surveillance Technologies
Challenges and Prospects for Strengthened Export Controls

Cryptography Export Controls
Testing the Dual-Use Concept

Issue 04

Strategic Trade Review

ISSN: 2506-9691
E-ISSN: 2406-5269

STR serves as an open source international forum for advanced exploration of the strategic trade field. STR's mission is to provide its readers with valuable resources regarding the current state of this area of study. STR pledges to publish articles of only the highest caliber that have gone through double-blind peer review and make them available to scholars and interested members of the public.

PUBLISHER
University of Liege
Place du 20-Août, 7
4000 Liège
Belgium

With support from the European Commission's Joint Research Centre and the University of Liege, European Studies Unit.

Contents

A Resilience Framework for Understanding Illicit Nuclear Procurement Networks

AARON ARNOLD[1]

Abstract

Current approaches to global supply-side controls to curb the proliferation of nuclear dual-use goods and technologies fail to consider the mechanisms that drive non-state actors to adapt and innovate. Consequently, policymakers are left reacting to, rather than anticipating, new illicit procurement techniques and methods. This article proposes a new analytical framework based on the concept of resilience, which considers how illicit procurement networks change and adapt within environments characterized by risk and uncertainty. That is, how do internal and external drivers help to insulate or create vulnerabilities for procurement networks? Focusing on the causes and consequences of resilience offers a more dynamic and comprehensive picture of illicit procurement because the concept can account for how networks adapt to supply-side policies and vice versa. To further illustrate this framework, this article explores three cases of illicit nuclear procurement. Finally, the conclusion examines the possible implications for future global supply-side policies to control the spread of nuclear dual-use goods and technologies.

Keywords:

Counter-proliferation, illicit procurement, resilience, nuclear

1 Aaron Arnold is an Assistant Professor at Curry College in Milton, MA. He is also an Associate at the Project on Managing the Atom, at Harvard University's Kennedy School of Government. Aaron spent ten years as a nonproliferation and counter-proliferation consultant to the United States Department of Defense, Department of Homeland Security, and the Department of Justice. His work primarily focuses on nuclear proliferation, threat finance, and sanctions evasion.

Introduction

Despite the successful conclusion of a nuclear agreement with Iran in late 2015—a deal that limits Iran's nuclear program in exchange for sanctions relief—the illicit global trade in nuclear and missile technology remains an active and ongoing concern. Globalized commerce, increased access to dual-use goods, growing indigenous manufacturing capabilities, and persistent demand for missile and nuclear technology have produced a niche market for middlemen to act as conduits between supplier and proliferator states.[2] Yet, despite global efforts to control the spread of dual-use goods and technologies, procurement networks are often able to operate under the radar of intelligence and law enforcement organizations. Iranian procurement networks, for example, were largely able to evade global efforts to limit Iran's nuclear enrichment program to increase its number of gas centrifuges, all while under strict international economic sanctions and virtually cut-off from the global financial system.[3] It should be noted, however, that while Iran was able to increase its number of gas centrifuges, the country was not able to make significant scientific progress on improving its uranium enrichment program, and generally continued to use the outdated IR-1 centrifuge design. Nonetheless, what explains the apparent persistence and success of nuclear procurement networks to continue operations given the increased attention to strengthening global supply-side controls?

The overall strategy of nuclear supply-side controls is to curb the transfer of "difficult-to-produce technology and equipment that is essential for making nuclear weapons and intended by the purchaser for that purpose."[4] This includes limiting trade in materials with both nuclear and non-nuclear applications, the timely detection of proliferation-related activities, dissuading proliferating-related activities, and disrupting or denying proliferation-related activities when

---

2 Bruno Gruselle, "Proliferation Networks and Financing," Fondation pour la Recherche Stratégique, Paris, 2007, p. 7, <http://www.stanleyfoundation.org/publications/working_papers/Delory5.pdf>. See also Matthew Bunn, Marty Malin, William Potter and Sandy Spector, *Preventing Black Market Trade in Nuclear Technology* (Cambridge: Cambridge University Press, forthcoming).

3 In 2006, the UN Security Council adopted resolution 1737, which banned exports to Iran of "all items, materials, equipment, goods, and technology" related to nuclear activities. The Security Council expanded this ban in March 2008 to include travel sanctions on specific individuals, as well as nuclear-related sanctions on entities affiliated with Iran's nuclear program. Finally, in June 2010, the Council imposed its most restrictive sanctions against Iran with resolution 1929, which prohibited Iran from investing in foreign nuclear activities, banned weapons exports to Iran, called on member states to inspect all cargo to and from Iran, expanded the list of sanctioned entities, and finally, called for states to implement additional financial-related sanctions. Despite these restrictions, Iran made progress on its nuclear enrichment program. In 2003, for example, Iran maintained a few hundred centrifuges, but by 2013, experts believed Iran's number of centrifuges had grown to over 19,000. Many of the items Iran procured, like carbon fiber, valves, and aluminum tended to be below-threshold items, which made it difficult for authorities to "identify links between below-threshold items and prohibited end-users and end uses in Iran." See, "Final Report of the Panel of Experts Established Pursuant to resolution 1929 (2010)," United Nations Security Council, June 2014, pp. 14–15, <http://www.un.org/ga/search/view_doc.asp?symbol=S/2014/394>; "Visualizing Centrifuge Limits Under the Iran Deal," *Nuclear Threat Initiative*, June 25, 2015, <http://www.nti.org/analysis/articles/visualizing-centrifuge-limits-under-iran-deal/>.

4 Matthew Bunn, Marty Malin, William Potter and Sandy Spector, *Preventing Black Market Trade in Nuclear Technology* (Cambridge: Cambridge University Press, forthcoming).

they occur.[5] These approaches, however, fail to account for the ability of procurement agents and networks to adapt. A motivated network will find ways to circumvent even the most rigorous controls. For the purposes of this article, a procurement network is taken to mean the networks of middlemen that either wittingly or unwittingly illicitly procure nuclear dual-use goods and technologies on behalf of a state. These networks can vary in size, scope, and sophistication; may be comprised of one or more members; and organized as a formal, business-like partnership, such as the A.Q. Khan network, or more informally, based on familial relationships. Iran, for example, has tended towards de-centralization with respect to procurement activities.[6] North Korea, on the other hand, has generally maintained a strong, centrally-directed network of procurement operations.[7] This definition is somewhat broader in scope than other definitions, which tend to focus on the state, its intentions, and its direct interactions with other proliferation aspirants.[8]

Interestingly, while supply-side controls make up a significant portion of the global nuclear nonproliferation regime, relatively little attention is given to the inner-workings of the procurement networks. Consequently, supply-side controls have trouble anticipating how procurement networks will adapt. This is not to imply that the controls are static. On the contrary, there is a clear evolution of global supply-side controls that has adapted to changes in the spread of nuclear goods and technologies. In response to India's 1974 nuclear weapons test, for example, nuclear supplier countries formed the Nuclear Suppliers Group (NSG) to develop and issue guidance on limiting the export of sensitive nuclear materials and technologies. Although the NSG is an informal multilateral export control arrangement between nuclear suppliers, with no legal authority or formal enforcement mechanisms, its participating governments have implemented its guidelines through national laws and practices. During the 1980s and 1990s, the United States called attention to the NSG's lack of specific guidance on controlling the exports of dual-use goods and technology (i.e., goods that have both nuclear and non-nuclear applications).[9] It was eventually the revelations of Iraq's covert nuclear program that helped

---

5 Andrew C. Winner, "The Proliferation Security Initiative: The New Face of Interdiction," *The Washington Quarterly* 28:2 (March 1, 2005), pp. 129–43; Frederick McGoldrick, "Nuclear Trade Controls: Minding the Gaps," CSIS, Washington, DC, January 2013, <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130122_McGoldrick_NuclearTradeControls_Web.pdf>.

6 For a short history of Iran's procurement activities, see, "Final Report of the UN Panel of Experts Established Pursuant to Resolution 1929 (2010)," S/2014/394, Annex II, June 2014, <http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2014_394.pdf>.

7 For a recent discussion on the scale and scope of North Korea's procurement operations, see John Park and Jim Walsh, "Stopping North Korea, Inc.: Sanctions Effectiveness and Unintended Consequences," MIT Security Studies Program, August 2016, <http://web.mit.edu/ssp/people/walsh/Stopping%20North%20Korea%20Inc_Park%20%20Walsh_FINAL.pdf>.

8 Chaim Braun and Christopher F. Chyba, "Proliferation Rings: New Challenges to the Nuclear Nonproliferation Regime," *International Security* 29:2 (October 1, 2004), pp. 5–49; Alexander H. Montgomery, "Ringing in Proliferation: How to Dismantle an Atomic Bomb Network," *International Security* 30:2 (October 1, 2005), pp. 153–87.

9 For further discussion of dual-use goods and technologies, see, "Communication Received from the Permanent Mission of the Republic of Korea to the International Atomic Energy Agency Regarding Certain Member States' Guidelines for Transfers of Nuclear-Related Dual-Use Equipment, Materials, Software and Related Technology," Information Circular, International Atomic Energy Agency, October 24, 2016.

usher in new NSG guidance on controlling dual-use technology.[10]

Later, responding to the threat of potential nuclear terrorism, the UN Security Council unanimously adopted resolution 1540 in 2004, which requires UN Member States to prohibit any support to non-state actors seeking WMDs, adopt and enforce laws that criminalize the proliferation of WMDs to non-state actors, and establish domestic controls over nuclear-related technologies, goods, and services.[11] While some states moved quickly to adopt and implement new supply-side controls, others still lag.[12]

The picture of global supply-side controls that begins to emerge is one that is left reacting to, rather than anticipating, nuclear procurement. Moreover, as export controls change and enforcement tightens, procurement networks iteratively change and adapt. That is, even as states moved to strengthen these controls globally, whether through interdictions, export control regimes, or sanctions, procurement channels and networks adapted. Middlemen have adopted a range of techniques and methods to hide their illicit activities, including transshipment through a third-party country, targeting countries with lax export controls to set up operations,

---

10 Fred McGoldrick, "Nuclear Trade Controls: Minding the Gaps," A Report of the CSIS Proliferation Prevention Program (Washington, DC: Center for Strategic and International Studies, January 2013). One of the key issues with dual-use technologies is its ubiquity among both nuclear and non-nuclear states. This, of course, is quite problematic for supply-side controls that mainly focus on controlling goods and technologies from supplier states. R. Scott Kemp argues, for example, that technology once thought to be "exotic" is now commonplace and accessible to even the most unsophisticated proliferation aspirants—either through indigenous capability or clandestine procurement. The implication, of course, is that policymakers should look beyond supply-side controls to the "cultural, normative, and political organization of the world" in order to reduce demand. Yet, despite Kemp's compelling argument, some proliferation aspirants, like Iran and North Korea, relied heavily on procuring complicated foreign technology, even when they had the capability (and opportunity) to indigenize. In the case of Iran, for example, Kemp argues that A.Q. Khan's contributions to Iran's gas centrifuge program in the late 1980s was insignificant. Interestingly, although Iran mastered the P-1 gas centrifuge design, the country continued to covertly procure foreign materials and parts. This, despite relatively sophisticated indigenous manufacturing. In other words, Iran may have viewed supply-side controls (including economic and financial sanctions) as so weak and incapable, that they posed no real threat to the advancement of its nuclear enrichment program. See, R. Scott Kemp, "The Nonproliferation Emperor Has No Clothes," *International Security* 38:4 (April 1, 2014), pp. 40–41.

11 In May 2003, then President George W. Bush announced the Proliferation Security Initiative (PSI), which seeks to enhance global coordination and collaboration with respect to WMD trafficking. More specifically, the initiative focuses on ensuring that participating countries have the national legal authorities to prohibit and prevent WMD proliferation, the ability to inspect and identify proliferation-related cargo, the ability to seize and dispose of interdicted materials and technologies, and the mechanisms in to ensure swift decision-making. Less than five months after its launch, in October 2003, the PSI had its first successful interdiction of a German-owned cargo ship carrying components for 1,000 centrifuges destined for Libya. It was this interdiction that began to unravel the extent of A.Q. Khan's network, and put into question the efficacy of global export controls. See "Chronology: A.Q. Khan," *The New York Times*, April 16, 2006, <http://www.nytimes.com/2006/04/16/world/asia/16chron-khan.html>.

12 "2016 Comprehensive Review: Background Paper for the Formal Open Consultations by the 1540 Committee," United Nations, New York, NY, June 22, 2016, p. 4, <http://www.un.org/en/sc/1540/pdf/CR-June-Consultation-Background-Paper.pdf>. Although the prevailing wisdom was that compliance with nonproliferation norms was a function of cost and the unequal distribution of benefits, Stinnett et al., for example, explain that states' non-compliance with UNSCR 1540 is more closely related to bureaucratic and economic capabilities, rather than national security interests. See, Douglas M. Stinnett et al., "Complying by Denying: Explaining Why States Develop Nonproliferation Export Controls," *International Studies Perspectives* 12:3 (August 1, 2011), p. 323.

obfuscating payments, forging end-user certificates and export licenses, and procuring "below threshold" components that may suffice or be upgraded by the recipient.[13] Part of A.Q. Khan's success, for example, was his ability to adapt procurement methods to evade scrutiny from both law enforcement and intelligence agencies worldwide. This included compartmentalization of key activities, the use of front companies, increasing the number of intermediaries, creating fraudulent end-user certificates, and conducting business through corrupted banks to obscure payments. For at least a while, Khan's nimble and adaptable network proved to be quite an obstacle for global export controls meant to curb illicit nuclear procurement.[14]

Counter-proliferation policies have evolved in such a way as to emphasize procurement *modus operandi* rather than underlying processes that may influence the *way* a network adapts and changes. Interestingly, the techniques and tactics that nuclear procurement networks use have changed very little. In fact, a 1984 de-classified US intelligence assessment on gray market nuclear materials highlights the frequent use of front companies, falsification of end-user certificates, alteration of information listed on export applications, and transshipment through third-party countries with lax export controls.[15] These methods are nearly identical to those described by the UN Panel of Experts' report on the implementation and violations of UN Security Council resolution 1929, which imposed stiff sanctions and embargoes on Iran.

This is not to suggest that addressing procurement methods is unimportant. On the contrary, a deep understanding of illicit procurement methods and techniques is necessary to close gaps in global export controls and strengthen enforcement mechanisms. Consider, however, the problem of proliferation financing—that is, the financing of illicit nuclear procurement. Unlike terrorist financing or money laundering associated with narcotics trafficking, proliferation financing often resembles normal trade finance—practically undetectable from the perspective of the financial industry.[16]

---

13 David Albright, Paul Brannan, and Andrea Stricker, "Detecting and Disrupting Illicit Nuclear Trade after A.Q. Khan," *The Washington Quarterly* 33:2 (April 1, 2010), pp. 85–106.

14 It is important to note that the Khan network was an outlier of sorts when compared to other states' entrenched procurement networks. Iran, for example, has demonstrated a keen ability to take a distributed approach, where its procurement agents rely extensively on middlemen located overseas—mostly in China. In these networks, illicit procurement revolves primarily around evading export controls, with little actual nuclear know-how. North Korea, on the other hand, uses an approach that more closely resembles a version of the A.Q. Khan network in terms of scale and complexity. In a recent study, John Park and Jim Walsh describe the complex and tangled system of "state trading companies," which the North Korean regime uses to conduct both licit and illicit procurement. See John Park and Jim Walsh, "Stopping North Korea, Inc.: Sanctions Effectiveness and Unintended Consequences," MIT Security Studies Program, August 2016, <http://web.mit.edu/ssp/people/walsh/Stopping%20North%20Korea%20Inc_Park%20%20Walsh_FINAL.pdf>.

15 "The Gray Market in Nuclear Materials: A Growing Proliferation Danger," An Intelligence Assessment, Washington, DC: Central Intelligence Agency, Directorate of Intelligence, July 1984, <https://www.cia.gov/library/readingroom/document/cia-rdp85t00287r000600940003-2>.

16 For a discussion of proliferation financing, see Sonia Ben Ouagrham-Gormley, "Banking on Nonproliferation," *The Nonproliferation Review* 19:2 (July 1, 2012), pp. 241–65; For an industry perspective of proliferation financing, and analysis of current issues with global counter-proliferation financing policies, see Emil Dall, Andrea Berger, and Tom Keatinge, "Out of Sight, Out of Mind? A Review of Efforts to Counter Proliferation Finance," Royal United Services Institute, June 2016, <https://rusi.org/publication/whitehall-reports/out-sight-out-mind-review-efforts-counter-proliferation-finance>.

Of course, one of the primary reasons for the gap in analysis is a lack of information on the internal workings of illicit procurement networks. Procurement is a secretive, covert activity, and the information that is available tends to be limited in scope. Although nuclear procurement networks share similar properties, they have varied in scope, scale, structure, and purpose.[17] This article takes a different approach. Rather than identifying new procurement techniques and tactics, this article proposes a new analytic framework, which uses the concept of resilience to explain illicit procurement networks' processes of innovation and adaptation within environments characterized by risk and uncertainty. That is, what are the mechanisms that allow networks to bounce back from some type of shock such as an enforcement action?

Resilience, within this context, is the product of underlying environmental, organizational, and individual-level factors. In other words, the ability of a procurement network to adapt or innovate is influenced by some basket of variables, like individual learning and level of street sense, organizational structure and access to resources, and understanding changes in external legal, political, social, or economic influences.

Understanding these interactions can provide fresh insights into difficult questions. How dedicated, for example, are illicit procurement channels and what is their degree of specialization? More specifically, how connected are middlemen to states' proliferation interests, or is it merely a case of opportunity and arbitrage? Is there crossover between legitimate and illicit markets and if so, to what extent? Is there competition within illicit procurement channels? If so, what are the consequences? What is the role, if any, of criminal deterrence? How do network members learn to defend against enforcement? How do middlemen interpret and understand export laws? How does enforcement influence decision-making within networks? From a policy perspective, resilience may help to enable policies that specifically target and inhibit the ability of procurement networks to bounce-back.

The next section describes the key parameters of resilience. Then, to illustrate how the framework may provide useful insights, three cases of illicit procurement are presented which help to illustrate the interplay between internal and external drivers and identify the attributes or qualities that enable a network to respond to external shocks. Alternatively, what attributes tend to neutralize enforcement actions? By no means are the cases representative of all types of illicit nuclear procurement, but they nonetheless provide an intuitive benchmark. It is also important to reiterate that the objective of this article is to provide an analytical framework that moves beyond a general discussion of *modus operandi* to a more nuanced understanding of internal network dynamics. In other words, the cases and subsequent discussion only demonstrate what amounts to a proof of concept and does not suggest confirmation of a causal mechanism.

Resilience: A New Approach to Understanding Illicit Procurement

The concept of resilience can have multiple meanings depending on the context and unit of analysis. On one hand, resilience is the ability of a system to bounce back to its original state.

17 Bruno Gruselle, "Proliferation Networks and Financing," Fondation pour la Recherche Stratégique, Paris, 2007, p. 7, <http://www.stanleyfoundation.org/publications/working_papers/Delory5.pdf>; Alexander H. Montgomery, "Ringing in Proliferation: How to Dismantle an Atomic Bomb Network," International Security 30:2 (October 1, 2005), pp. 153–87.

At the other end of the spectrum, resilience is the ability of a system to adapt and evolve into a new state in response to unforeseen external shocks.[18]

Originally used to describe phenomena within ecological systems, resilience has gained popularity in recent decades to understand the capacity of social systems to deal with uncertainty and risk.[19] After the 9/11 terrorist attacks, the organizational sciences and consequence management fields found resilience to be a useful construct to describe the ways organizations bounce back from low probability, high impact events. Practitioners and scholars have also applied similar frameworks to describe how criminal and terrorist networks adapt to disruptions stemming from enforcement or regulatory actions, changes in network dynamics, or changes in market dynamics.[20] Others have even suggested resilience as a way to strengthen global nonproliferation norms.[21]

Resilience is defined in this article as the general capacity of a network to evade or bounce back from external or internal disruptions. External disruptions may be environmental disruptions, such as increased enforcement actions, or changes in domestic law. Internal disruptions, on the other hand, might include breakdowns in communications or loss of operating revenue. In other words, it is a foolhardy task to assume that a procurement network's success or failure is determined solely on the success or failure of supply-side controls. This is true in part, but discounts the persistence of nuclear procurement networks in the face of counter-proliferation efforts aimed at shutting them down. The ability of a procurement network to evade and adapt to government enforcement and supply-side controls is a sign of its resilience. However, resilience is not constant, and not all networks bounce back or succeed in evading efforts to disrupt their operations.

Identifying sources of resilience within networks, let alone illicit networks, is a relatively nascent field. In a study on illicit drug networks, however, Martin Bouchard provides a useful definition of resiliency as a function of three key attributes: vulnerability, elasticity, and adaptability.[22]

Vulnerability is a network's relative exposure to internal or external threats. For example, how compartmentalized are the network's activities compared to the relative level of enforcement? Reducing vulnerability, however, is not necessarily an intrinsic or an automatic process. It requires forethought and critical evaluation of potential and likely threats. Take, for example, organization and logistics, which are oftentimes points of vulnerability for illicit procurement. A

---

18 Karl Weick, "Introductory Essay: Improvisation as a Mindset for Organizational Analysis," *Organization Science* 9:5 (October 1, 1998) pp. 543–55; Louise K. Comfort, Arjen Boin, and Chris C. Demchak, eds., *Designing Resilience: Preparing for Extreme Events* (Pittsburgh, Pa: University of Pittsburgh Press, 2010), p. 8.

19 Aaron B. Wildavsky, *Searching for Safety* (New Brunswick, USA: Transaction Books, 1988).

20 Julie Ayling, "Criminal Organizations and Resilience," *International Journal of Law, Crime and Justice* 37:4 (December 2009), pp. 182–96; Martin Bouchard, "On the Resilience of Illegal Drug Markets," *Global Crime* 8:4 (November 1, 2007), pp. 325–44.

21 Arian Leigh Pregenzer, "Systems Resilience: A New Analytical Framework for Nuclear Nonproliferation," Sandia National Laboratories, December 1, 2011, <http://www.osti.gov/scitech/biblio/1034890/>.

22 Martin Bouchard, "On the Resilience of Illegal Drug Markets," *Global Crime* 8:4 (November 1, 2007), pp. 325–44.

network that is reliant on a single mode of shipping is more vulnerable than a network that uses multi-modal transport systems. It is important to note, however, that vulnerability is contextual, and often dependent on other environmental factors. Whereas using multi-modal logistics and shipping systems may reduce vulnerability in regions where export enforcement is high, it may have no effect in areas where export enforcement is low—thus, an inefficient use of resources. Alternatively, a network that employs several shipping partners and routes simultaneously where enforcement is high may also increase its risk of detection and interdiction. Therefore, reducing vulnerability consists of an interplay between external forces and internal network responses.

Whereas vulnerability characterizes overall exposure to threats, elasticity characterizes the network's ability to "bounce back" from unforeseen shocks and return to its original state. If a key member is extricated from the network, how does the network recover functionality? Redundancy, for example, is a key component to elasticity. Duplicate communications systems can help mitigate against a shock that may neutralize one or more channels. However, redundancy, in and of itself, may not be entirely sufficient to ensure elasticity. In a centralized network that lacks compartmentalization, for example, redundant communication networks may offer no protection against external surveillance. Under this scenario, redundancy may provide law enforcement and intelligence agencies even greater access to the inner workings of the network.

It is important to note, however, that elasticity does not necessarily imply that the network is easily able to adapt. If the shock is too great, and the network cannot bounce back, it must either adapt or perish. Bouchard defines this capacity to adapt as, "…the extent to which [the network] can modify its circumstances to make its components less vulnerable."[23] Of course, adaptation can be a complex process and over time requires a great deal more resources to be successfully achieved. In the case of illicit procurement, adaptation may mean using new smuggling routes, finding alternate suppliers, changing corporate identities, substituting goods, or moving operations to a new location altogether. It is also important to note that an adaptation may involve something entirely new and yet to be discovered by intelligence, law enforcement, or regulatory authorities.

Vulnerability, elasticity, and adaptability are not mutually exclusive elements of resilience. A resilient network can, and oftentimes does, display properties of each element. Sometimes they are complementary, and sometimes they are competing. Reducing vulnerability by compartmentalizing information, for example, may decrease overall elasticity or even the capacity to adapt. Restricting access to information or people may demonstrate a keen awareness of a need for greater security, but it can also inhibit information flows during periods of crisis. Likewise, a network may be able to increase its elasticity by increasing its number of members or modalities, but it is quite possible that in doing so, the network increases its vulnerability to outside scrutiny by offering more access points.

The next sections will describe how organizational, individual, and environmental factors affect resilience. To better illustrate the proposed relationship between resilience and environmental, organizational, and individual factors, Figure 1 illustrates a notional path diagram, which shows how exogenous factors (organizational, environmental, and individual) affect endogenous factors of resilience (vulnerability, elasticity, and adaptability).

23 Ibid, 330.

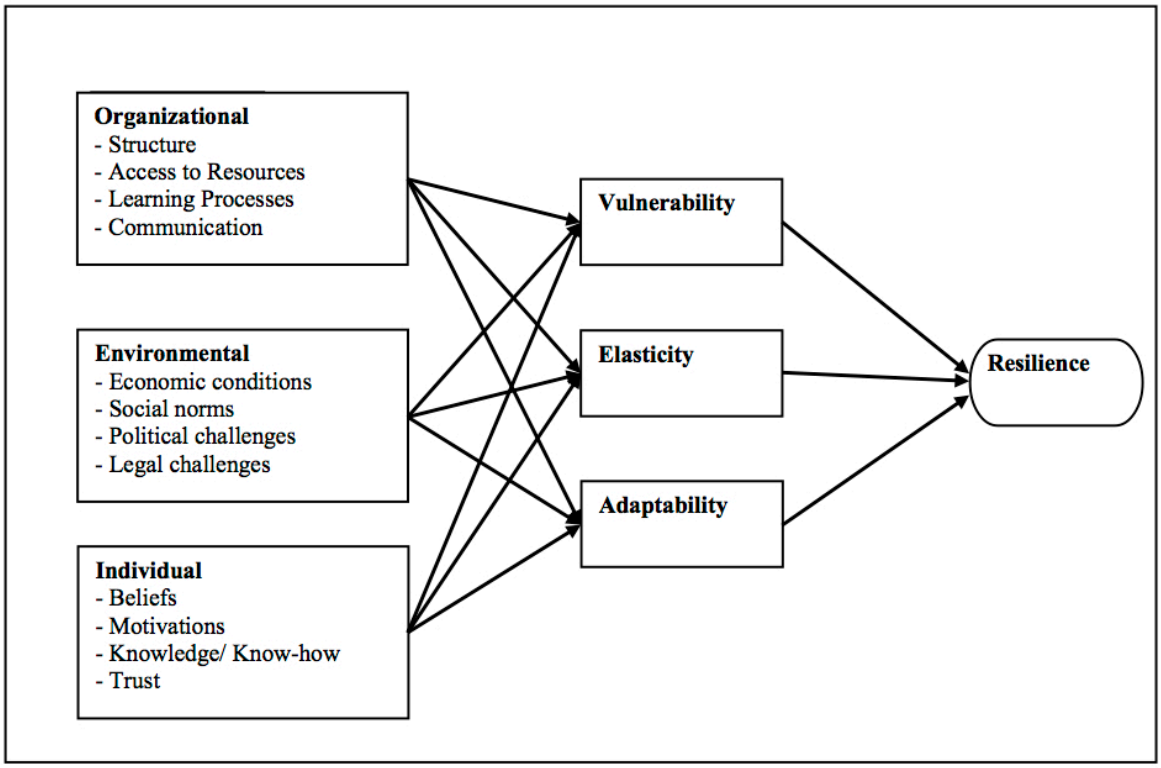

Figure 1. Notional Path Diagram of the Relationship between Resilience and Organizational, Environmental, and Individual Factors

Organizational and Individual Factors

Generally, organizational and individual level factors are the intrinsic characteristics of the network. At the organizational level, structure, access to resources and learning processes can all affect the elasticity, vulnerability, and adaptability of a network. Likewise, individual level factors, such as communication, beliefs, and motives can also affect resilience in similar ways.[24]

Take technical expertise, for example. Within illicit procurement networks, technical expertise, which is a function of information availability and learning, can play an integral role in guarding against shocks and maintaining core functionality. The degree to which procurement agents understand the technology they are dealing with has the potential to either mitigate or exacerbate external threats. On one hand, if members of the network have a strong technical background, they may be better suited to identify relevant suppliers. If a supplier is cutoff, technical expertise may prove useful in finding not only alternative suppliers, but alternative materials. Technical expertise may also insulate against certain types of law enforcement actions, like undercover operations, where fake or dummy materials are used.

Interestingly, trust dynamics—an individual level factor comprised of belief systems and motives—between network members may also play an important role for resilient networks. A

24 Diane L. Coutu, "How Resilience Works," *Harvard Business Review* 80:5 (May 2002), pp. 46–55; Arjen Boin and Michel J. G. van Eeten, "The Resilient Organization," *Public Management Review* 15:3 (March 1, 2013), pp. 429–45.

network that enjoys a high degree of trust is able to adjust quickly to external or internal threats, as information is more easily transferred among members.[25] In a recent study on trust dynamics within a nuclear smuggling network, Egle Murauskaite described the process within a loosely connected network.[26] The author suggests that the overall lack of deep trust, either based on familial bonds or repeated transactions, may have increased the network's susceptibility to infiltration—thus reducing resiliency.[27]

Likewise, A.Q. Khan's eventual undoing was the CIA recruitment of key network members. In 2003, intelligence agencies pressured Friedrich Tinner and his sons—key members of the Khan network who helped transfer material and know-how to Libya—to turn against Khan.[28] In this case, the breakdown in trust and loyalty among key members was too much for the network to recover from. It may also indicate that Khan himself was not fully aware of the security concerns his network faced from intelligence agencies, and therefore did not think to address those vulnerabilities.

Learning and sense-making is also a critical driver within resilient networks. In general terms, learning and sense-making are the processes that organizations and organizational members use to accumulate and synthesize information.[29] It is important to realize, however, that organizational and individual level factors may have different effects (or roles to play) within illicit networks than they do in legitimate networks. Traditional notions of organizational learning, for example, present peculiar problems for illicit networks. Take for example learning through trial and error. While the opportunity costs of trial and error are high for any organization, it may be impossibly high for illicit networks. Illicit networks always run the risk of erring on the first trial, which may have catastrophic consequences. Secrecy presents another challenge, as the accumulation of tacit knowledge may be tempered by the need for greater secrecy and compartmentalization within procurement networks.

Flexible organizational structures may also promote the ability to act creatively and innovate under ambiguous or uncertain conditions—further contributing to resilience. In illicit networks, redundancy, de-centralization, and loose-coupling between nodes are all factors

---

25 Cynthia Stohl and Michael Stohl, "Networks of Terror: Theoretical Assumptions and Pragmatic Consequences," *Communication Theory* 17:2 (May 1, 2007), pp. 93–124.

26 Egle Murauskaite, "The Trust Paradox in Nuclear Smuggling," *The Nonproliferation Review* 22:3–4 (October 2, 2015), pp. 321–39.

27 Ibid, 333–34.

28 David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies* (New York: Free Press, 2010), p. 10.

29 Although complex, there are three general processes that describe how organizations learn: experience accumulation, knowledge articulation, and knowledge codification. The first, experiential accumulation, occurs through a process of environmental interactions, whereby the interactions lead to the accumulation of tacit knowledge. Learning by doing and learning through trial and error are simple examples. Knowledge articulation occurs when organizations figure out what works and what does not work through sharing and communication among organizational members or groups within an organization. Finally, knowledge codification happens when the organization formalizes what it learned through the creation of blueprints, manuals, and standard operating procedures. See, for example, Chris Argyris and Donald Schon, *Organizational Learning: A Theory of Action Perspective* (Reading, MA: Addison-Wesley, 1978); James G. March, "Exploration and Exploitation in Organizational Learning," *Organization Science* 2:1 (February 1991), pp. 71–87. Maurizio Zollo and Sidney G. Winter, "Deliberate Learning and the Evolution of Dynamic Capabilities," *Organization Science* 13:3 (June 1, 2002), p. 341.

that can minimize the impact of external disruptions.[30] The need for secrecy, however, tends to promote compartmentalized structures. While compartmentalization may create obstacles for efficient legitimate organizations, it can reduce the impact of a compromised or damaged node within an illicit network by reducing the probability of catastrophic cascading effects. The A.Q. Khan network, for example, effectively compartmentalized sensitive activities and used redundant structures through a complex network of shell and front companies.[31] Therefore, taking out a single intermediary generally did not have profound consequences throughout the rest of the system.

Finally, access to economic resources affects the capacity to innovate and pursue creative solutions. A recent report by C4ADS and the Asian Institute for Policy Studies notes that North Korea's overseas procurement networks are largely successful due to their access to significant State resources.[32] In particular, the report highlights the case of Dandong Hongxiang Industrial Development Co. Ltd., which is a North Korean procurement front that conducts over $500 million in trade annually, including trade in dual-use goods with military and nuclear applications.[33] Greater access to working capital ensures that illicit networks are able to easily change identities or shift operations to new locations when under threat.

Environmental Factors

Illicit procurement networks must also contend with environmental drivers, such as competition from other illicit networks, local policies and laws, enforcement actions, social and political conditions, market structure, and changes in demand.[34] These factors, of course, can impose significant costs or benefits, either forcing the network to adapt or insulating the network against vulnerability. In some respects, these are all responses to increased risk and uncertainty within the network's operating environment such as increased global awareness of proliferation risks and implementation of supply-side controls.[35]

---

30 Julie Ayling, "Criminal Organizations and Resilience," *International Journal of Law Crime and Justice* 37:4 (December 2009); Jacqueline Brewer and Michael Miklaucic, *Convergence: Illicit Networks and National Security in the Age of Globalization* (Washington, DC: National Defense University Press, 2013), pp. 213–33; Mark S. Granovetter, "The Strength of Weak Ties," *American Journal of Sociology* 78:6 (May 1, 1973), pp. 1360–80; Cynthia Stohl and Michael Stohl, "Networks of Terror: Theoretical Assumptions," Communication Theory 17:2 (May 2007); Arjen Boin and Michel J. G. van Eeten, "The Resilient Organization," *Public Management Review* 15:3 (March 1, 2013), pp. 429–45.

31 David Albright, Paul Brannan, and Andrea Stricker, "Detecting and Disrupting Illicit Nuclear Trade after A.Q. Khan," *The Washington Quarterly* 33:2 (April 1, 2010), pp. 85–106.

32 "In China's Shadow: Exposing North Korean Overseas Networks," Asian Institute for Policy Studies, Washington, DC, August 2016, <http://en.asaninst.org/contents/in-chinas-shadow/>.

33 Ibid, 34.

34 Julie Ayling, "Criminal Organizations and Resilience," *International Journal of Law Crime and Justice* 37:4 (December 2009).

35 Many of Iran's procurement activities highlight this phenomenon. Consider the case of the Islamic Republic of Iran Shipping Lines (IRISL)—an entity subjected to US and EU sanctions since 2008 and 2010, respectively, due to its role in supporting Iran's nuclear and ballistic missile programs. IRISL illustrates how financial and insurance sanctions, for example, can induce adaptation and result in system resilience. As sanctions increased, IRSL adapted by re-flagging and renaming its shipping vessels, tampering with end-user certificates, and adjusting information to conceal financial transactions in order to maintain access to global financial systems. See "Update on the Continuing Illicit Finance Threat Emanating from Iran," Department of the Treasury Financial Crimes Enforcement Network, Washington, DC, June 2010.

Enforcement actions can be a strong motivating factor in promoting illicit procurement networks to adapt. In fact, as Michael Kenney points out, the interaction between enforcement and internal forces can lead to a process of "competitive adaptation," whereby networks adapt to external forces and vice-versa.[36] As "players" are eliminated and enforcement strategies change, the net result is a more efficient system with a higher state of resiliency.

Changes within the networks' political, social, or economic environment may also enable success or failure by bolstering or hindering resiliency. Although US and international sanctions against Iran exacted significant economic damage, the sanctions also bolstered its resilience to external shocks. A recent report by John Park and Jim Walsh on the efficacy of sanctions against North Korea found that they were largely ineffective at stopping North Korean procurement. In fact, the report goes on to claim that sanctions may have even increased Pyongyang's procurement capabilities.[37] According to the authors, North Korean procurement firms were able to successfully monetize risk as sanctions drove up transaction costs.

In Iran's case, it is quite clear that international sanctions fomented social and political acceptance of sanctions-busting networks, which enforced resiliency in two ways. First, acceptance provides a sense of security. The efficacy of Iran's procurement networks was, in part, bolstered a widespread belief in the illegality of international sanctions, which led to the legitimization of illicit procurement networks. "Of course we bypass sanctions. We are proud that we bypass sanctions because the sanctions are illegal," commented Iranian President Hasan Rouhani about US and international sanctions.[38] Evading sanctions, then, became a patriotic duty of sorts.[39]

In 2016, a prominent Iranian-Turkish businessman—Reza Zarrab—was implicated in a fraudulent scheme of bribery and corruption to control a gold smuggling operation that provided Iran access to foreign currency. According to a criminal indictment filed in the Southern District of New York, from about 2010 to 2015, Reza Zarrab operated multiple money service businesses located in the United Arab Emirates and Turkey which he knowingly allowed Iranian banks to use in order to evade US sanctions.[40] In 2011, for example, Zarrab instructed Al Nafees Exchange, which is a UAE-based exchange house, to make international payments on

---

36 Michael Kenney, *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation* (University Park, Pa: Pennsylvania State University Press, 2007), p. 108.

37 John Park and Jim Walsh, "Stopping North Korea, Inc.: Sanctions Effectiveness and Unintended Consequences," MIT Security Studies Program, August 2016, <http://web.mit.edu/ssp/people/walsh/Stopping%20North%20Korea%20Inc_Park%20%20Walsh_FINAL.pdf>.

38 "Iran President Rouhani Hits out at US Sanctions," *BBC News*, August 30, 2014, sec. Middle East, <http://www.bbc.com/news/world-middle-east-28997452>; "Iran President Condemns US Sanctions 'Invasion,'" *The Associated Press*, August 2014.

39 See for example Peter Andreas, "Criminalizing Consequences of Sanctions: Embargo Busting and Its Legacy," *International Studies Quarterly* 49:2 (June 1, 2005), pp. 335–60; R. T. Naylor, *Patriots and Profiteers: Economic Warfare, Embargo Busting, and State-Sponsored Crime* (Montreal: McGill-Queen's University Press, 2008).

40 USA v. Rezza Zarrab, Indictment S1 15 Cr. 857 (US District Court, Southern District of New York May 2016).

behalf of Mellat Exchange—a subsidiary company of the Iranian Bank Mellat.[41] In a December 2011 letter to the general manager of Iran's central bank, Zarrab wrote that, "The role of the Supreme Leader and the esteemed officials and employees of Markazi Bank play [*sic*] against the sanctions, wisely neutralizes the sanctions and even turns them into opportunities by using specialized methods."[42] He then goes on to suggest that it is his "national and moral duty" to evade global sanctions.

In March 2012, for example, the European Union cut off Iran's access to the Society for Worldwide Interbank Financial Telecommunications (SWIFT).[43] The SWIFT-ban, coupled with the US financial sanctions, ousted Iran from the global financial system, and almost overnight, Iranian firms found themselves without a means to access global markets. Iranian firms, however, could adapt and eventually return to normal operations—albeit with higher transactions costs—in part by displacing operations to new locations and finding new payments routes. In some cases, these payment routes moved into less regulated and opaque financial centers, such as the United Arab Emirates. Ultimately, Iranian businesses began to normalize smuggling techniques such as using transshipment points in Dubai, falsifying end-use certificates, exploiting loopholes in remittance regulations, and co-opting regional neighbors.

In fact, it is likely that this level of normalization and legitimization of smuggling provided redundancy and increased resilience for Iran's nuclear procurement operations. As international sanctions increasingly cut Iran off from global trade and commerce, nuclear and ballistic missile procurement and sanctions evasion became increasingly interlinked—relying on the same logistic and financial intermediaries.

Finally, state demand for dual-use goods and technology may play a significant role. One of the more significant unaddressed questions regarding illicit nuclear procurement is the role and effect of market competition. How much, if any, competition exists between illicit procurement networks? If so, how do networks manage this competition? This dynamic creates somewhat of a paradox in nuclear procurement. From one angle, proliferator states may want to increase the chances of successful procurement by promoting multiple supply networks. While this may increase the resiliency of procurement operations from the perspective of the proliferator state, the added competition may increase the vulnerability of the individual procurement agent. How, then, do procurement agents deal with this inherent tension?

The next section describes three recent cases of illicit nuclear procurement. By no means are these cases representative of every type of illicit nuclear procurement network, but each

---

41 The US Department of the Treasury, Office of Foreign Assets Control (OFAC) added Bank Mellat to the Specially Designated Nationals list in October 2007, pursuant to Executive Order 13382—an executive order that targets proliferators of WMDs. According to the Treasury Department, Bank Mellat provided banking and other financial services to entities involved in Iran's nuclear program, such as the Atomic Energy Organization of Iran. As part of the Joint Comprehensive Plan of Action, the United States removed its sanctions against Bank Mellat in January 2016.

42 USA v. Rezza Zarrab, Indictment at 10, S1 15 Cr. 857 (US District Court, Southern District of New York May 2016). Bank Markazi is Iran's central bank.

43 Headquartered in Belgium, SWIFT provides a secure network infrastructure for banks to send transaction-related information, is the world's largest global financial messaging service.

offers unique perspectives that help illustrate the dynamics of using a resilience framework—specifically the interplay between internal and external drivers. The data for each case is primarily derived from court transcripts, as well as other public records, including government reports and periodicals.

Case I: Nicholas Kaiga

Between September 2007 and June 2013, Belgian national Nicholas Kaiga worked as an intermediary to procure and transship dual-use and nuclear export controlled materials to Iran. According to the criminal indictment against Kaiga, an unnamed co-conspirator located in Iran submitted multiple orders to a named US company for aluminum tubing, which listed the end-user as *Super Alloys*—a company located in the United Arab Emirates.[44] A short investigation by a US export control officer found that an Iranian company with ties to sanctioned entities owned *Super Alloys*. Shortly thereafter, the US Bureau of Industry and Security denied the export license for the aluminum.

To avoid export licensing requirements, *Super Alloys* requested that the US company begin shipping non-export controlled materials to a purported customer in Belgium—*Industrial Metals & Commodities SPRL* (IMC), which listed Nicholas Kaiga as the owner and operator of the company. By 2009, US Immigration and Customs Enforcement began an undercover operation against *Super Alloys*. As the investigation continued, it became evident that Kaiga was re-shipping materials to a front company in Malaysia, which the unnamed Iranian co-conspirator also owned. From Malaysia, the materials were forwarded on to the UAE and then re-exported to Iran.

To determine the ultimate end-user, undercover agents shipped sham aluminum to Kaiga in December 2011, which Kaiga then forwarded to Malaysia and eventually on to Iran in February 2012.[45] Eventually, Kaiga contacted the undercover agent to inquire about the authenticity of the materials. ICE arrested Kaiga in July 2013. He was found guilty of committing violations of the International Economic Emergency Powers Act and sentenced to 27 months in prison. In July 2015, the United States deported Nicholas Kaiga back to Belgium.

Although successful in his procurement, at least initially, Kaiga is at best characterized as an unsophisticated middleman who took advantage of export control gaps. One notable feature about Kaiga's network is its structure. It was the simplicity of his network, at least in part, which reduced his overall vulnerability. In a sense, by keeping its membership low, he could reduce his vulnerability to enforcement actions. In fact, according to court records, the undercover agent made several overtures to Kaiga, asking to join his operations—which Kaiga refused.

---

44 The aluminum tubing in this case, which was 7075 T6 aluminum, has aerospace and nuclear applications. The specialized aluminum can be used to manufacture gas centrifuges, and is therefore export controlled. See, USA v. Nicholas Kaiga, Criminal Complaint (US District Court, Northern District of Illinois, Eastern Division 2013).

45 Although it is clear from the indictment that Kaiga and the co-conspirator had a business relationship, it is not clear whether or not Kaiga was aware of the ultimate destination of the materials that he was transshipping to Malaysia. It is clear, however, that Kaiga was aware that he was violating export control laws by transshipping the restricted goods to Malaysia.

Although it is possible that he balked at this offer out of an abundance of caution, it is more likely that Kaiga did not see a legitimate business need to expand his operations. In other words, business was slow for Kaiga.

Although he lacked technical expertise regarding the parts he was acquiring, Kaiga was a skilled businessman with a strong background in international financing and banking. He understood European Union export laws, which he could leverage in order to re-export controlled goods to Malaysia. Unfortunately for Kaiga, his lack of technical expertise ultimately left him vulnerable to an undercover operation led by US Immigration and Customs Enforcement.

During the undercover operation, ICE agents sent Kaiga dummy aluminum tubes. Believing the parts were genuine, Kaiga then forwarded the tubes on to Malaysia, where they were re-exported to Iran. It was only after they reached Iran when Kaiga learned that the order did not meet the correct specifications. Interestingly, even when he did find out they were dummy tubes, he thought the US manufacturer was at fault—he did not once consider that he may be the subject of an undercover operation. Had Kaiga identified the dummy tubes, he could have cut his losses and displaced his activities elsewhere. Of course, Kaiga had no reason to believe that he was under investigation. Unlike other cases, however, the United States did not add Kaiga to its sanctions list. If it had, perhaps he would have been more cautious—even seeking alternative methods to obscure his identity.

At best, Kaiga's network could be characterized as inelastic and vulnerable to external enforcement. Most notably, Kaiga's lack of redundant systems left his operations open to infiltration. Furthermore, if Kaiga had a better technical understanding of the materials he was dealing in, he might have become aware of US interest in his operations much sooner—giving him time to find alternative suppliers.

Case II: Sihai "Alex" Cheng

In January 2016, Sihai "Alex" Cheng was sentenced to nine years in prison for violating US export control laws. According to the criminal indictment, between 2009 and 2012, Cheng—a Chinese citizen—worked with Iranian national Seyed Jamili to procure and transship thousands of export controlled pressure transducers, worth almost $2 million, to Iran.[46] Cheng and Jamili met at a trade show in Guangzhou, China. It was at this meeting where an enterprising Cheng agreed to work with Jamili to acquire sensitive components that would ultimately end up in Iran's gas centrifuge program. In fact, without Cheng's involvement, it is quite unlikely that Jamili could procure the parts.[47] Shortly after Cheng's indictment, the United States and European Union sanctioned Jamili's company, *Eyvaz Technic*, for its involvement with Iran's nuclear program.

---

46 Pressure transducers are sensors with multiple applications, but can be used to measure pressure during uranium enrichment processes. Indictment in the case of the United States of America v. Sihai Cheng, No. 13CR10332 (n.d.).

47 USA v. Sihai Cheng, Sentencing Hearing Transcript (US District Court for the District of Massachusetts 2016).

Cheng's network appears to have been quite unique in that it is one of the few known recent cases where corrupted employees of a supplier took part in the illicit activity. Employees at a Shanghai-based subsidiary of MKS Instruments, which is a parts supplier based in Andover, Massachusetts, worked with Cheng to obtain fraudulent export licenses.[48]

One of the keys to Cheng's early success was his ability to compartmentalize information and thus maintain at least some degree of secrecy. Email records from Cheng's sentencing hearing suggest that he kept most of his co-conspirators in the dark about the most sensitive aspects of his operations. In fact, in an email to Jamili, Cheng wrote, "I must tell you again, the goods are supplied to us secretly. MKS doesn't know it's supplied to me. They think it's supplied to the Shanghai agent and used for some Chinese solar energy and semiconductor industry…"[49] Hu Johnson—another co-conspirator—believed that the items were being re-exported to Singapore—genuinely unaware that the parts were ultimately destined for Iran.[50]

Cheng's degree of technical expertise was quite low. In fact, even though it was clear that Cheng knew he was committing export violations, it is unclear whether he knew the parts were intended for Iran's nuclear program. Not only did Cheng not have a solid understanding of the technical aspects of the parts he was procuring, but his international business acumen was lacking as well.[51] His attorney, however, notes that while Cheng is quite intelligent, his knowledge of international business is quite naive.[52] This lack of expertise may have contributed to an inability to guard against external shocks. A superficial understanding of international business can limit an actor's ability to find alternative payment schemes, new logistic routes, or substitute suppliers. It also means the actor may not be attuned to changes in demand or regulatory and legal requirements. Ultimately, then, the lack of business acumen puts Cheng's illicit operations in jeopardy and reduces overall resiliency. It is important to note, however, that although Cheng may not have been an international trade expert, it is not possible to measure the direct effect of his inexperience on his overall success or failure with illicit trade.

One aspect of Cheng's operations that clearly impacted his network's vulnerability and elasticity was his belief that he would not be caught (i.e., sense-making). Cheng maintained that he

---

48 Indictment in the case of the United States of America v. Sihai Cheng; David Albright and Andrea Stricker, "Case Study - Chinese Salesman Arrested in Pressure Transducer Case," Institute for Science and International Security, Washington DC, January 18, 2013, <http://isis-online.org/isis-reports/detail/case-study-chinese-salesman-arrested-in-pressure-transducer-case/>.

49 "Sentencing Memorandum in the Case of the United States v. Sihai Cheng" (US District Court of Massachusetts, February 1, 2016), p. 45.

50 In a statement before the court, Cheng provides a different account, noting that he did in fact tell the MKS employees that the pressure transducers were for an end-user in Iran. See, USA v. Sihai Cheng, Sentencing Hearing Transcript at 145. In a related case, however, the US Government noted that there is no evidence that Qiang Hu knowingly caused export controlled parts to be shipped to Iran. See, USA v. Qiang Hu, Government Sentencing Memorandum (United States District Court, District of Massachusetts 2014).

51 Cheng graduated with an English degree from Shandong University, and shortly thereafter began working in international trading, which was lucrative and provided income for his family, who are farmers rural provinces of Goungzhou.

52 USA v. Sihai Cheng, Sentencing Hearing Transcript at 163. While profit was a strong motivator for Cheng, his attorney noted that it was more the excitement of being involved in a global business and the corresponding prestige. Nonetheless, Cheng himself admits that his motivations were based on greed.

perceived the risk of getting caught to be low and that he did not fully realize the severity of his export violations.[53] Although some evidence suggests that Cheng at least partially understood the severity of his export violations, he nonetheless openly traveled to London, where he was arrested and eventually extradited to the United States. This suggests that Cheng was not aware of impending law enforcement actions against him and his network.[54]

Finally, Cheng's access to resources, specifically working capital, was quite limited. In fact, for most of his procurement, Jamili fronted Cheng the cash to complete each transaction. While the US prosecutors contend that Cheng worked to procure almost $2 million worth of parts for Iran's nuclear program, Cheng's profit margin was quite narrow. Although the exact amount is unknown, he likely split about $450,000 between 13 co-conspirators over a five-year period. In other words, Cheng was taking a significant risk for what amounted to a few thousand dollars a year. Thus, without significant proceeds, Cheng did not have the resources to reduce his network's vulnerability by maintaining multiple front companies, bank accounts, and logistic routes. Had his operations been more lucrative, perhaps Cheng would have taken greater precautions to insulate his network from external threats.

Overall, Cheng's resiliency was rather low. Low working capital, no back-up systems, and no expectation of getting caught meant that Cheng was not prepared when the United States decide to enforce export controls.

Case III: Li Fang Wei

Li Fang Wei, better known as Karl Lee, controls one of the most enigmatic procurement networks since A.Q. Khan. For more than a decade, Li—a Chinese procurement agent—has been a "principal supplier" to both Iran's ballistic missile and nuclear programs.[55] Unfortunately, other than information obtained from US criminal indictments, as well as a blurry picture on a FBI Wanted poster, not much is known about Li. What is known, however, is that Li runs one of the largest procurement channels since the Khan network and yet enforcement agencies have been unable to shut his operations down. In fact, he is currently the only procurement agent with a $5 million bounty for information leading to his arrest. Unlike the two previous cases, however, Li is known not just for his ability to act as a middleman, but also as a manufacturer. In fact, a recent analysis of his network suggests that Li may be manufacturing and exporting sensitive guidance components, which have ballistic missile applications.[56]

---

53 Emails between Cheng and Jamili seem to indicate that Cheng knew of the risks he was taking by transshipping the export controlled items to Iran. In one email Cheng wrote, "Time is important, not only for you, for me, for your end-user, but also for your nation. I personally believe the war will break out in two years, and that will be the start of World War III." It should be noted, however, that during the sentencing hearing, Cheng offered a different explanation for this exchange, suggesting this was merely "bravado" meant to entice and keep Jamili as a customer. In fact, other evidence does suggest that Cheng became increasingly concerned that Jamili would cut him out of the procurement operations.

54 According to a person familiar with the case, the Chinese government may have tipped-off Cheng to the United States' interest in his business operations. Despite this warning, however, Cheng continued his procurement operations.

55 David Albright, Andrea Stricker, and Donald Stewart, "Serial Proliferator Karl Li," Institute for Science and International Security, Washington DC, May 8, 2014, <http://isis-online.org/isis-reports/detail/serial-proliferator-karl-li-chinas-continued-refusal-to-act/20>; Daniel Salisbury and Ian Stewart, "Wanted: Karl Lee" Project Alpha, King's College, London, UK, May 19, 2014, <http://projectalpha.eu/wanted-karl-lee/>.

56 Ibid.

The internal workings of Li's network are largely a mystery to outsiders. But, over the last decade, Li has made extensive use of front companies and circuitous financial transactions in order to obscure his illicit dealings—techniques that go well beyond what Kaiga and Cheng employed. In 1998, Li first established *LIMMT Economic and Trading*—a company Li used to transfer relatively large quantities of high-end carbon fiber and aluminum alloys to Iran. In 2006, the US Treasury Department added *LIMMT* to its sanctions list, and later, in 2009, added Li himself.[57]

To evade sanctions, Li established a complex network of front companies and aliases. Between 2004 and 2014, Li used over a dozen fronts and even more aliases. In fact, Li would often use family members or business associates to obscure his true identity from banks.[58] Unlike the other networks, however, Li has been able to quickly bounce back from external shocks and even adopt new methods. In fact, one of the major drivers of Li's adaption were US law enforcement and regulatory actions. When the US added Li's front companies to the Treasury Department's sanctions list, he changed his corporate identities. When the FBI seized Li's assets through his Chinese bank's US correspondent accounts, he simply moved his remaining assets into financial institutions with no US correspondent accounts.

Another factor bolstering Li's resilience is that his expectation of interference from Chinese enforcement is quite low. In fact, some evidence suggests that the Chinese government had warned Li about possible impending US sanctions. Not surprisingly, the Chinese have refused multiple extradition requests, despite multiple dèmarches from the US State Department.[59]

Clearly, Li's operations are far more resilient than Kaiga and Cheng. Two significant factors likely helped bolster this resilience. First, US sanctions against Li and his companies provided a signal to Li that he needed to adapt or else face possible criminal or economic penalties. In other words, it was the US designation that tipped-off Li, and then Li's ability to interpret—or make sense of—this signal to come up with clever evasion methods. Second, Li has a large pool of capital at his disposal. Thus, he can afford maintenance costs associated with running multiple front companies.

Discussion and Implications

The Nicholas Kaiga, Alex Cheng, and Karl Li cases each illustrate that resilience within procurement networks is a varied process, influenced—at least in part—by internal and external drivers. It is important to note, however, that these cases only demonstrate what amounts to a proof of concept, and does not suggest evidence of causal mechanism. That is, while many of the findings are quite intuitive, the cases are rather narrow and will require additional analysis using further cases. Moreover, these cases focused specifically on Iranian nuclear procurement. North Korea, for example, uses very different methods. Nonetheless, even as a proof of concept,

57 In Rem Complaint against Karl Lee, No. 14 CIV (Southern District of New York April 29, 2014).

58 Daniel Salisbury and Ian Stewart, "Wanted: Karl Lee" Project Alpha, King's College, London, UK, May 19, 2014, <http://projectalpha.eu/wanted-karl-lee/>.

59 "NIAG 8233: Transfer of Maraging Steel from China to Iran," Wikileaks Public Library of US Diplomacy, Secretary of State, January 14, 2009, <https://wikileaks.org/plusd/cables/09STATE3943_a.html>.

these findings do have implications for global supply-side controls from both a policy and enforcement perspective.

First, it is important to note that the model, as described in this article, cannot, with any degree of certainty, make the claim that some controls are better able detect or dissuade a network in a specific resilient state. Clearly, this is a logical conclusion, which might lead one to believe that enforcement of supply-side controls should consider ways to reduce a network's overall resilience or prevent a network from achieving a higher state of resilience. Yet, the research is not yet at a point to make this determination. To make this determination, a more thorough analysis of the covariation between successful operations and factors of resilience is needed.

Some of the findings, however, do suggest that access to resources may play an important role in network resilience. In April 2014, a federal grand jury indicted Li, *in absentia*, for sanctions violations and money laundering. Instead of attempting to shut him out of the global financial system by imposing sanctions, the Justice Department targeted Li's assets. Interestingly, the Justice Department employed a seldom used tactic against Li entailing the filing of a civil complaint against Li's assets. In doing so, the US Government could seize his assets which were held in overseas accounts at Bank of China and Shanghai Pudong Development Bank by seizing funds from the banks' accounts in the US.[60] In doing so, the US Government was able to seize almost $7 million of Li's assets. It is important to note, however, that the process of competitive adaptation ensures that Li, and others like him, will work to insulate themselves against this type of enforcement in the future. Thus, agencies must be willing to innovate and seek out new strategies.

A resilience framework may also offer recommendations to improve policy approaches to global export control regimes. Take, for example, the illicit financing of nuclear procurement. One of the key challenges for banks and government agencies in detecting financial transactions relating to nuclear procurement is the inability to identify specific patterns of behavior—also "activity-based" proliferation finance. The financial industry is quite adept at conducting name and entity checks against international sanctions and export-control lists, but less so at detecting patterns. A recent report on proliferation financing by the Royal United Services Institute found that banks need a better understanding of the underlying "behavioral signatures of the illicit procurement."[61] Understanding the persistent ability of nuclear procurement networks to adapt—its resilience—might be able to help bridge this problem. Of course, to do so, US intelligence and enforcement agencies must overcome obstacles that prevent efficient and transparent information sharing with the private sector.

A new area of research with significant implications for export control policy is on non-state proliferator motivations. Why would an intermediary in China be willing to transship export controlled materials to Iran and risk potential fines, or even worse, arrest and incarceration? Conventional wisdom assumes that middlemen are largely profit-motivated and weigh these incentives against the costs of getting caught. Although the risk versus reward calculus can be

60 In Rem Complaint against Karl Lee, No. 14 CIV (Southern District of New York April 29, 2014).

61 Emil Dall, Andrea Berger, and Tom Keatinge, "Out of Sight, Out of Mind? A Review of Efforts to Counter Proliferation Finance," Royal United Services Institute, June 2016, <https://rusi.org/publication/whitehall-reports/out-sight-out-mind-review-efforts-counter-proliferation-finance>, p. 26.

rather parsimonious for policy makers, the evidence available tends to demonstrate that profits are quite low and the risks of detection by law enforcement and intelligence agencies is not trivial. In fact, it seemed to be the case that in the Cheng and Kaiga cases, each viewed the risk of getting caught as so low that even minimal profits were worth the risk. While perhaps counterintuitive, this is consistent with some of the criminological literature on why people commit crimes.[62] To be sure, however, a much deeper analysis is necessary to determine these causal mechanisms.

Of course, understanding these motivations is important when considering possible deterrent effects. In sentencing Alex Cheng, for example, it was quite clear that the judge was interested in sending a deterrent message to potential export violators. In justifying the lengthy prison sentence, the judge noted that, "…there are a lot of people there who are trying to get our stuff out of the country into other countries. So it's not so much him [Cheng]. You have to have a serious deterrent."[63] Here, the judge assumed—perhaps wrongly—that a lengthy sentence imposed against Cheng would send a deterrent signal to other would-be procurement agents.

In a new article by Ian Stewart and Daniel Salisbury, which explores non-state actor motivation, the authors state that, "For an actor to be deterred, the potential perceived cost of the action must outweigh the benefit."[64] This, of course, implies that certainty over severity can be a de-motivator for procurement agents. But, a resilience framework would suggest some level of adaptation. When enforcement does increase, for example, the net result is likely a more lucrative market for proliferators. In other words, risk can be monetized within illicit procurement, which may in turn attract new procurement actors.[65]

Conclusion

Nuclear weapons aspirants, historically, have at least partially relied on acquiring foreign materials and technology to support enrichment programs. Given this trend, coupled with a

---

62 Take, for example, the routine activities theory of crime, which postulates that motivation, abundance of opportunity, and the lack of some type of macro-level control leads to criminal activity. While contentious, it nonetheless explains certain crimes, such as intellectual property theft and other types of occupational crimes. Recent work by Bichler and Malm applies routine activities theory of crime to explain motivation in transnational criminal activity—such as import/export violations. The authors explain how the lack of macro-level economic, social, political, and legal controls—especially in areas of jurisdictional asymmetry—coupled with globalized commerce and increased access to communications creates opportunity ripe for exploitation regardless of reward. For a discussion of the routine activities theory of crime, see Derek B. Cornish and Ronald V. Clarke, *The Reasoning Criminal: Rational Choice Perspectives on Offending* (New York, NY: Springer New York, 1986), pp. 1–16; see, also Gisela Bichler and Aili Malm, "The Routine Nature of Transnational Crime," in *The Criminal Act: The Role and Influence of Routine Activity Theory*, ed. Martin Andresen and Graham Farrell (New York, NY: Palgrave Macmillan, 2015), pp. 33–58.

63 "Sentencing Memorandum in the Case of the United States v. Sihai Cheng,", p. 167.

64 Ian Stewart and Daniel Salisbury, "Non-State Actors as Proliferators: Preventing Their Involvement," *Strategic Trade Review* 2:3 (Autumn 2016), p. 12.

65 For a discussion of the monetization of risk within illicit procurement see John Park and Jim Walsh, "Stopping North Korea, Inc.: Sanctions Effectiveness and Unintended Consequences," MIT Security Studies Program, August 2016, <http://web.mit.edu/ssp/people/walsh/Stopping%20North%20Korea%20Inc_Park%20%20Walsh_FINAL.pdf>.

long-held belief that the acquisition of complex technology remains the primary challenge for states seeking nuclear weapons, policymakers have focused much attention on controlling the spread of nuclear-related materials and technologies.[66] Unfortunately, this attention has come at the cost of ignoring other dimensions of illicit procurement.

The mesh of treaties, national laws, sanctions, embargoes, and non-binding political commitments tends to fall short of a seamless and integrated system capable of detecting and stopping illicit nuclear procurement. Ubiquitous technology and indigenization of manufacturing present significant challenges for global export regimes. Moreover, implementation gaps in United Nations Security Council resolution 1540 still present obstacles for transparency and capacity-building efforts. This article proposes a new framework based on the concept of resilience to better understand the core drivers that affect and promote illicit procurement. That is, despite efforts to stem the global trade in dual-use goods and technology, how are illicit procurement networks able to defend themselves, bounce-back, and adapt?

The three case studies presented help to paint a picture of how resilience can be used to analyze illicit procurement networks. What is clear is that knowledge acquisition, structure, learning, sense-making, innovation, and access to resources—in addition to external forces—can all influence the network's ability to adapt. Consequently, enforcement and policy must take proactive, rather than reactive, approaches to countering non-state proliferation of dual-use goods and technologies.

Acknowledgments

Special thanks to Martin Malin, Daniel Salisbury, Matt Bunn, and Robert Shaw for their guidance and comments on earlier versions of this paper.

66 R. Scott Kemp, "The Nonproliferation Emperor Has No Clothes," *International Security* 38:4 (April 1, 2014), pp. 39–78; Douglas M. Stinnett et al., "Complying by Denying: Explaining Why States Develop Nonproliferation Export Controls," *International Studies Perspectives* 12:3 (August 1, 2011), pp. 308–26; Frederick McGoldrick, "Nuclear Trade Controls: Minding the Gaps," CSIS, Washington, DC, January 2013, <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130122_McGoldrick_NuclearTradeControls_Web.pdf>; Matthew Kroenig, *Exporting the Bomb: Technology Transfer and the Spread of Nuclear Weapons* (Ithaca: Cornell University Press, 2010).

Chemical and Biological Contract Manufacturing Services: Potential Proliferation Concerns and Impacts on Strategic Trade Controls

JULIE A. CARRERA*, ANDREW J. CASTIGLIONI*, AND PETER M. HEINE[1]

Abstract

The use of contract manufacturing services in the chemical, pharmaceutical, and biotechnology industries has grown significantly in recent years, but the potential for such service providers to be exploited for chemical or biological weapons proliferation has garnered relatively little attention, despite the role of contract manufacturers in the A.Q. Khan nuclear proliferation network. This article examines the dual-use potential and global spread of chemical and biological contract manufacturing and their ramifications for related strategic trade controls (STCs). Hundreds of providers of dual-use contract services were found worldwide, but they were primarily located in jurisdictions with comprehensive STC regulations. This provides some degree of protection against their misuse. However, the results outlined below also suggest that chemical and biological contract manufacturers are a critical community to target for STC outreach activities and efforts to increase industry compliance. Targeted outreach would help prevent contract manufacturing service providers from unwittingly contributing to the production and proliferation of chemical and biological weapons.

Keywords

Australia Group, Chemical Weapons Convention, contract manufacturing, CW precursors, dual-use chemical technology, dual-use biotechnology, pathogens, toxins, strategic trade controls, export controls

1 Julie A. Carrera is Section Manager and Principal Chemist for the Chem/Bio Analysis Section in the Center for Strategic Security. She has been a proliferation and trade analyst at Argonne for over a decade, with a focus on chemical weapons issues. Andrew J. Castiglioni is a Principal Biologist and a Proliferation and Trade Analyst in the Chem/Bio Analysis Section in the Center for Strategic Security. He held research positions in academia and industry prior to joining Argonne as a technical expert on biological weapons nonproliferation. Peter M. Heine is the Director of the Center for Strategic Security.

* These authors contributed equally to this manuscript.

Introduction

Contract manufacturing—i.e., contractual engagement of a third-party provider to generate a product—has become an increasingly attractive option over the last decade for chemical, pharmaceutical, and biotechnology companies seeking to reduce costs and operate competitively in a business environment characterized by increasing regulation, dwindling product approval, and rapidly advancing technology. In the chemical sector, contract manufacturers enable increased manufacturing capacity and flexibility without large capital investments by those requiring the service, as well as access to synthetic and process expertise that may not be available in-house and management of safety and regulatory issues. For the pharmaceutical and biotechnology sectors, contract services lower drug discovery risks for larger companies and provide flexible, ready access to highly trained technical expertise. Significant cost efficiencies can be realized through many dimensions of contract manufacturing, including greater control by tertiary pharmaceutical companies over how they concentrate or offload their investment in expertise and equipment, although it should be noted that not all processes can be scaled up or contracted out with similar success. Current estimates place the number of chemical contract manufacturers in the thousands, and pharmaceutical and biotech contract manufacturers at over 500 worldwide—and rapidly growing.[2,3]

Contract manufacturing firms and service providers have received some attention in the context of chemical weapons (CW) and biological weapons (BW) proliferation, but relatively little attention in the context of strategic trade controls (STCs), despite exploitation of contract manufacturing by A.Q. Khan's nuclear proliferation network.[4,5] One notable article from 2012 addressed the importance of STC awareness for the pharmaceuticals contracting industry, but focused primarily on the legal and regulatory framework with which companies needed familiarity.[6] A 2014 United States National Academy of Sciences report on chemical manufacturing equipment highlighted shifts to contract manufacturing in the pharmaceutical industry as a potential source of concern, but only in the context of trade controls over the surplus dual-use equipment generated by outsourcing rather than how the contract services provided by these companies could be exploited for proliferation.[7]

---

2 "Chemical Information Services." ContractMFG database alone has 2,000 custom manufacturers. See <https://chemicalinfo.com/services/contractmfg/>.

3 *Contract Manufacturing in Pharmaceutical Industry, 2015–2025* (Vancouver: Roots Analysis, 2015), p. 22.

4 Charles D. Lutes, "New Players on the Scene: A.Q. Khan and the Nuclear Black Market," 2008, <http://iipdigital.usembassy.gov/st/english/publication/2008/08/20080815121848xjyrrep0.1191522.html#axzz4KFVWTxgx>.

5 "Designation of A.Q. Khan and Associates for Nuclear Proliferation Activities," US Department of State, 2009, <http://www.state.gov/t/isn/115913.htm>.

6 Eric McClafferty and Brooke Ringel, "Export Controls and the Biotech Industry: Are You in Compliance?," *Contract Pharma,* May 4, 2012, pp. 98–103.

7 Kathryn Hughes and Joe Alper, rapporteurs, *The Global Movement and Tracking of Chemical Manufacturing Equipment: A Workshop Summary,* Washington, DC: The National Academies Press, 2014, <http://www.nap.edu/catalog/18820/the-global-movement-and-tracking-of-chemical-manufacturing-equipment-a>.

This article explores the CW or BW proliferation potential posed by contract manufacturing service providers and possible ramifications for STC implementation. This is accomplished through an illustrative survey of companies providing dual-use chemical or biological contract services—i.e., a service that has legitimate commercial applications but that could also be exploited toward producing a CW or BW agent by producing or processing controlled CW precursors, pathogens, or toxins. Services for both production of materials and their refinement are investigated, since a proliferator may seek to split the overall process among providers to conceal their activities. The distribution of these companies across countries according to their Australia Group (AG) membership status and the comprehensiveness of their national control lists as of October 2016 are used to assess a basic level of proliferation risk. These findings are analyzed, in turn, to determine potential adverse consequences for STCs and how they might be mitigated.

For the purposes of this article, the term "contract manufacturing" or "contract services" will be used to describe any arrangement in which a third-party company is engaged in producing or processing chemical or biological materials on demand via some type of contract. In sectors that use these types of arrangements, a broader array of terminology is used to distinguish the terms of a given agreement. For example, a "toll manufacturing" arrangement typically involves a company (the customer) supplying raw materials and paying a toll (fee) to have another company manufacture a product; the toll manufacturer effectively rents its facility and equipment, and the customer is responsible for materials and process specifications.[8] In contrast, a contract manufacturer may source raw materials as well as provide facilities and equipment, creating a custom-made product for an individual customer. A "contract manufacturer" may be referred to as a "custom manufacturer," and both terms are sometimes used interchangeably with the term "toll manufacturer."[9] Of further note, competition and additional market forces on the pharmaceutical/biotech sectors have been pushing contract manufacturers to operate collectively as umbrella service companies, offering all services from initial research and development to production and manufacturing under one roof. Thus, the terms "contract development and manufacturing organization" and "contract research and manufacturing services" are increasingly becoming part of the contract manufacturing lexicon.[10] While differences in contractual arrangements and number of services offered could have ramifications for the level of proliferation risk, such differentiation is beyond the scope of this article. To avoid confusion regarding these nuances in terminology, all companies in this article are referred to as contract service providers.

---

8 Sierra Coating Technologies, LLC, "Toll Manufacturing versus Contract Manufacturing," 2015, <http://www.sierracoating.com/toll-manufacturing-versus-contract-manufacturing/>.

9 SOCMA, "Types of Specialty Chemical Manufacturers," 2016, <http://specialtymanufacturing.socma.com/specialty-manufacturers>.

10 *Contract Manufacturing in Pharmaceutical Industry, 2015–2025* (Vancouver: Roots Analysis, 2015), p. 23.

Results and Discussion

Chemical Contract Services

The primary contract services of potential CW proliferation concern are those involving chemical synthesis, particularly for key precursors that would be subject to STCs and scrutiny by responsible suppliers. In addition, contract distillation or other purification-related services, which are sometimes offered independently of custom synthesis, may be of interest. Therefore, a survey was conducted of companies capable of custom synthesis using CW-relevant chemistries, as well as those providing contract distillation or purification services.

Custom Synthesis

Providers of organophosphorus chemistries and chlorination and fluorination reactions were investigated for this study. Such reactions are relevant to the synthesis of advanced precursors for nerve and blister agents found in Schedule 2 of the Chemical Weapons Convention (CWC) and on the AG Common Control List (CCL) of CW Precursors.[11,12] Denying proliferators access to Schedule 2 chemicals can be an effective chokepoint given their relatively moderate commercial availability and their chemical similarity to CW agents. A database of custom manufacturers covering 2,000 companies in over 55 countries was searched for companies providing related reactions, and search results were displayed using the graphic visualization software Tableau.[13] The database was used to achieve a representative sampling of contract service providers, such that the results reported herein should be considered illustrative—not exhaustive—of the overall provider landscape. Companies were analyzed according to specific reactions of dual-use concern, as well as whether they are in a country that is a member of the AG. In addition, it was assessed whether the country or economy in which the company is located has an export control list that adheres to the AG CCL of CW Precursors; for those locations outside of AG membership, adoption of an EU-style dual-use list or a national list matching the AG CW precursor list as of 2014 was considered as a proxy for adherence to the list.[14] It is important to note, however, that all locations identified in this study are States Parties to the CWC except for Israel and Taiwan. States Parties to the CWC are bound to never "assist, encourage or induce, in any way, anyone to engage in any activity prohibited to a State

---

11 Organization for the Prohibition of Chemical Weapons, "Annex on Chemicals," Chemical Weapons Convention, <https://www.opcw.org/chemical-weapons-convention/annexes/annex-on-chemicals/>.

12 The Australia Group, "Export Control List: Chemical Weapons Precursors," 2015, <http://www.australiagroup.net/en/precursors.html>.

13 "ContractMFG," Chemical Information Services, <https://chemicalinfo.com/services/contractmfg/>.

14 That is, prior to the 2015 addition of diethylamine (DEA) to the AG list, to account for reasonable lags in the legislative process to update national control lists. The most recent addition of chemicals to the list prior to DEA was 2009, giving adequate time for the regulatory process to catch up by 2014 in those countries committed to following the AG list.

Party" under the treaty and are subject to its transfer provisions for scheduled chemicals.[15,16] Further, the CWC definition of chemicals weapons includes precursors for toxic chemicals, i.e., Article II, 1(a) "Toxic chemicals and their precursors, except where intended for purposes not prohibited under this Convention, as long as the types and quantities are consistent with such purposes."[17] As such, no State Party should assist the development or production of chemical weapons through supply of CW precursors. However, national implementing legislation for the CWC varies considerably among States Parties. While an analysis of the detailed status of such legislation in each country was not undertaken for this study, an OPCW report on the implementation of the CWC in 2014 cited 114 States Parties—only 60%—as having legislation "covering all initial measures for the implementation of Article VII."[18] Therefore, the establishment of a comprehensive dual-use export control list that includes AG-listed chemicals, rather than CWC membership, was taken as a benchmark for this study.

Figure 1 displays search results summarizing companies offering organophosphorus chemistries of potential relevance to CW precursor production, grouped by location and AG membership status. Company numbers represent distinct counts by company name in a given country or economy; some companies have multiple locations, and some provide multiple relevant reaction types of concern, but these were not distinguished for the purpose of this analysis. Results indicate that a strong majority of organophosphorus chemistry providers are located in AG member countries: 150 compared to 56 in non-member locations, or 73%. The United States has the largest number of providers, exceeding the country with the next largest count, India, by more than a factor of two.

15 Organization for the Prohibition of Chemical Weapons, "Article I. General Obligations," Chemical Weapons Convention, <https://www.opcw.org/chemical-weapons-convention/articles/article-i-general-obligations/>.

16 Organization for the Prohibition of Chemical Weapons, "Annex on Implementation and Verification," Chemical Weapons Convention, <https://www.opcw.org/chemical-weapons-convention/annexes/verification-annex/>.

17 Organization for the Prohibition of Chemical Weapons, "Article II. Definitions and Criteria," Chemical Weapons Convention, <https://www.opcw.org/chemical-weapons-convention/articles/article-ii-definitions-and-criteria/>.

18 Organization for the Prohibition of Chemical Weapons, "Report of the OPCW on the Implementation of the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction in 2014," <https://www.opcw.org/fileadmin/OPCW/CSP/C-20/en/c2004_e_.pdf>. The report on implementation in 2015 cites 148 States Parties with "relevant legislation" but with no similar comment on the comprehensiveness of those countries' legislation. Organization for the Prohibition of Chemical Weapons, "Report of the OPCW on the Implementation of the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction in 2015," <https://www.opcw.org/fileadmin/OPCW/CSP/C-21/en/c2104_e_.pdf>.

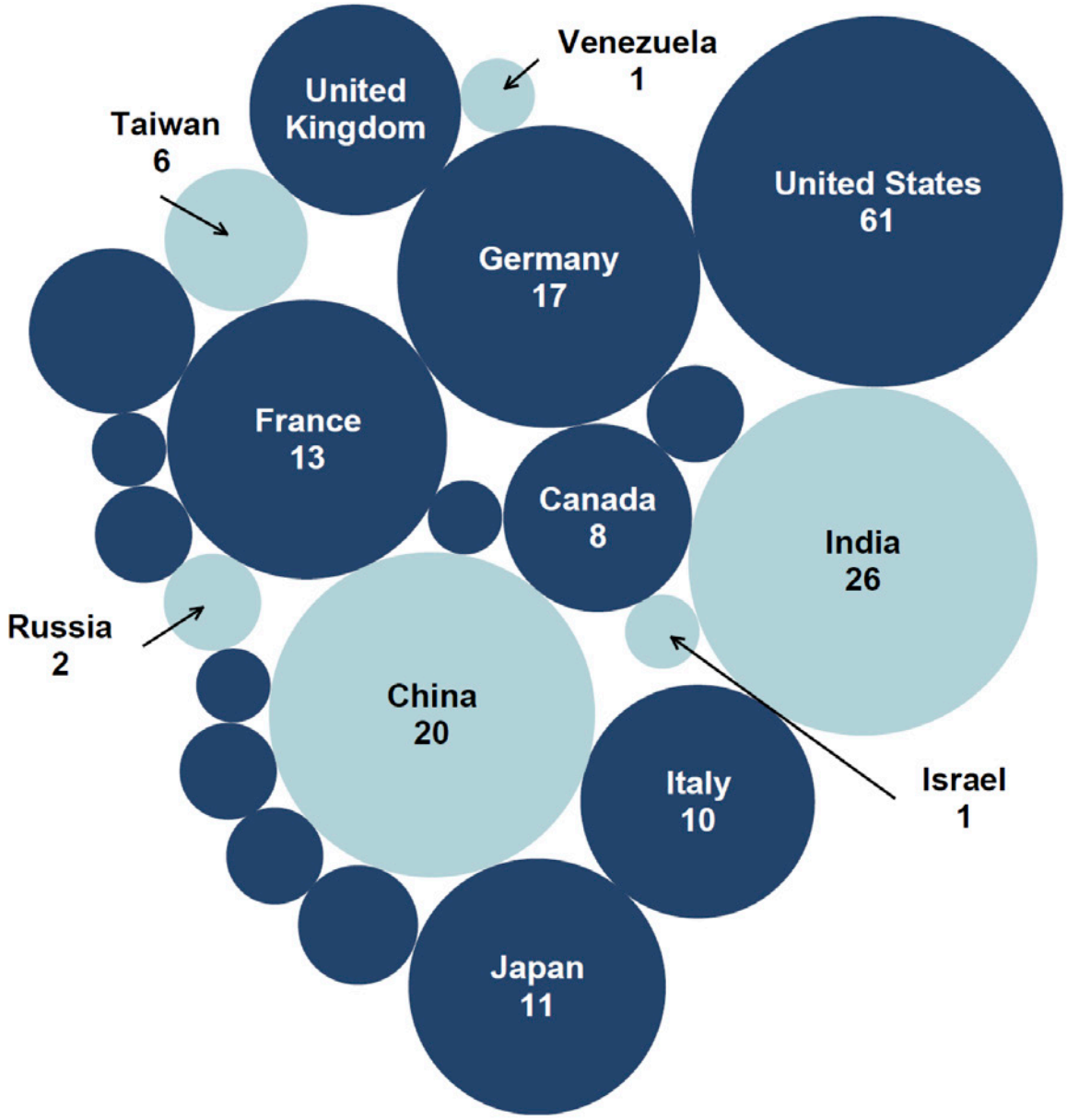

Figure 1. Number of companies offering CW-relevant organophosphorus chemistries, grouped by location and AG membership status. Circle diameter qualitatively represents the count of distinct company names in each location. AG members are indicated by dark blue, with non-members in light blue. A complete listing of countries and number of resident companies is provided in the Appendix (Table A1).

Examining the distribution of companies by fidelity to the AG CCL of CW Precursors (Figure 2) shows an even greater percentage of companies whose exports of listed precursors would likely be subject to national trade controls. Only one company out of the 206 found is in a country whose national control list does not adhere in part or in full to the AG list. Furthermore, while India's and China's national export control lists only partially cover the AG CW precursor

control list, they are comprehensive with respect to CWC scheduled chemicals. Therefore, any CWC scheduled organophosphorus compound synthesized by a company on their soil would be subject to national STCs.[19]

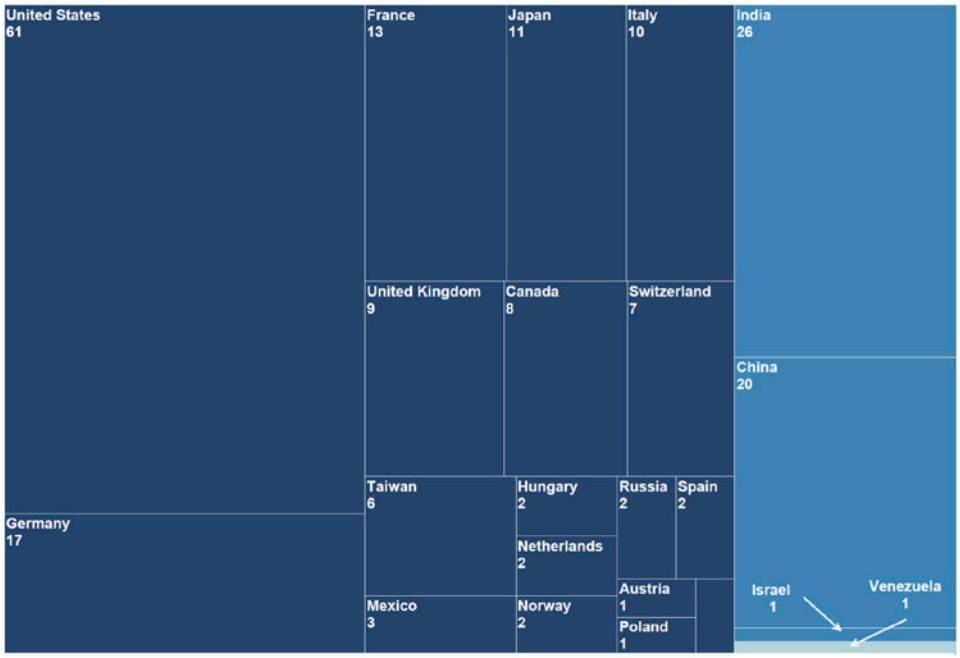

Figure 2. Number of companies offering CW-relevant organophosphorus chemistries, grouped by location and adherence to the AG CW precursor control list. Rectangle size represents the count of distinct company names in each location. Full adherence is indicated by dark blue. Partial adherence is indicated by medium blue. Non-adherence is indicated by light blue and includes only one country (Venezuela). A complete listing of countries and number of resident companies is provided in the Appendix (Table A2).

Similar analyses were conducted for chlorination and fluorination services. Figure 3 shows distinct company counts grouped by location and AG membership status. There is a substantially larger number of companies offering these reactions compared with organophosphorus chemistries: 526 distinct companies vs. 206 companies. In the case of chlorination and fluorination, the majority of providers are still in AG member countries, but only 56%. The balance changes somewhat when the individual reaction types are analyzed separately. The three reactions considered were fluorination, chlorination, and thionyl chloride ($SOCl_2$) reactions, the last being a method of chlorination.

19 This analysis is necessarily list-based, although neither the CWC Schedules nor the AG precursor list include all possible chemicals of CW proliferation concern. However, an analysis of the status of catch-all control provisions in national legislation is beyond the scope of this article.

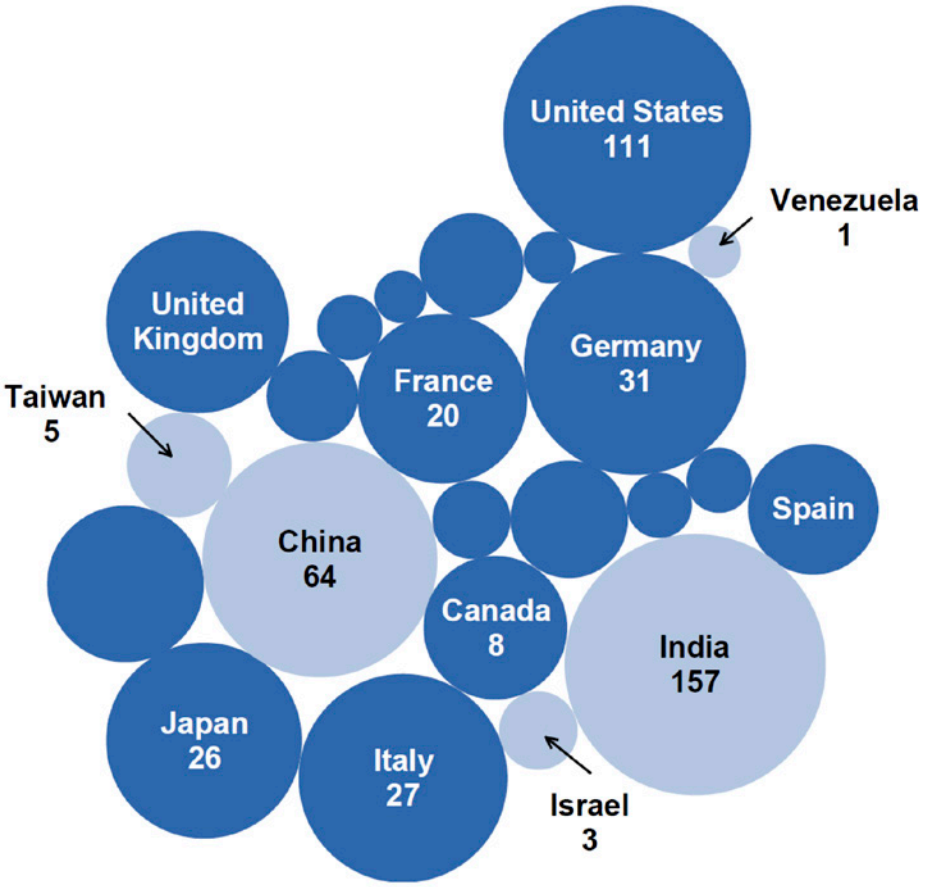

Figure 3. Number of companies offering CW-relevant chlorination and fluorination chemistries, grouped by location and AG membership status. Circle diameter qualitatively represents the count of distinct company names in each location. AG members are indicated by dark blue, with non-members in light blue. A complete listing of locations and number of resident companies is provided in the Appendix (Table A3).

As shown in Table 1, fluorination is less commonly provided than chlorination (204 vs. 475 companies) and is more concentrated in AG member countries (67% for fluorination vs. 56% for chlorination). $SOCl_2$ reactions are provided by few companies in the database used for this investigation, and those companies show a nearly even split between AG members and non-members. Figure 4 shows the distribution of companies by adherence to the AG CCL of CW Precursors. Again, only one company is in a country that does not adhere in part or in full, but the proportion of companies in partially adherent countries is substantially larger than for organophosphorus chemistry providers. India's and China's controls over CWC scheduled chemicals would again provide regulatory control over any scheduled chemicals resulting from custom chlorination or fluorination, although there are some AG-listed compounds that would not have been covered by those countries' lists at the time of the research conducted for this article.[20]

20 As of October 2016. Namely, 2-chloroethanol (107-07-3), dimethylamine hydrochloride (506-59-2), and triethanolamine hydrochloride (637-39-8). Other unscheduled, AG-listed compounds containing chlorine or fluorine are basic chemicals unlikely to be provided by contract synthesis providers (e.g., sodium fluoride).

AG Member	Location	Chlorination	Fluorination	SOCl2 Reactions
Yes	Austria	3		
	Belgium	5	3	
	Canada	8	4	
	France	19	9	1
	Germany	27	15	1
	Hungary	2		
	Italy	27	7	
	Japan	23	13	
	Mexico	4	1	
	Netherlands	2	1	
	Norway	1		
	Poland	5		1
	Portugal	1	1	
	South Korea	2	1	
	Spain	7	1	
	Switzerland	15	7	1
	United Kingdom	22	10	1
	United States	94	63	
No	China	50	40	
	India	149	23	6
	Israel	3	1	
	Taiwan	5	3	
	Venezuela	1	1	

Table 1. Number of companies offering CW-relevant chlorination and fluorination chemistries, grouped by AG membership status, location, and reaction.

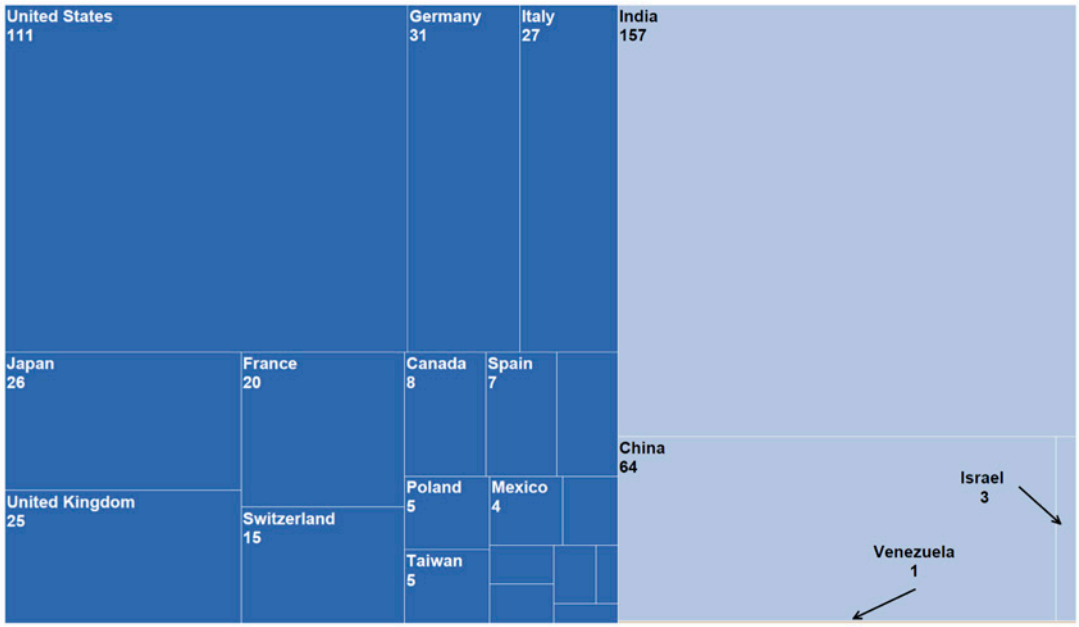

Figure 4. Number of companies offering CW-relevant chlorination and fluorination chemistries, grouped by location and adherence to the AG CW precursor control list. Rectangle size represents the count of distinct company names in each location. Full adherence is indicated by dark blue. Partial adherence is indicated by light blue. Non-adherence is indicated by gray and includes only one country (Venezuela). A complete listing of locations and number of resident companies is provided, see Appendix Table A4.

Distillation and Purification-Related Services

A survey was also conducted of companies providing custom or toll distillation; custom purification; or other purification, separation, or filtration services. The website of each company, when available, was reviewed to assess the potential for the company's services to be used for isolating significant quantities of dual-use chemicals of CW concern. Companies separating only laboratory-scale amounts and/or processing benign chemicals were considered of limited relevance for dual-use activities, while companies with corrosion-resistant equipment and/or citing work with harsh (and/or explicitly dual-use) chemicals were considered likely to be relevant. Companies reporting use of all-stainless-steel equipment that provided little detail about chemicals processed were considered potentially relevant, while some companies published insufficient information to determine the extent of their capabilities. While stainless steel is not considered sufficiently corrosion-resistant to be a specified material of construction in the AG CCL of Dual-Use Chemical Equipment, it could be exploited for a one-time purification operation of some CW-relevant chemicals.

A total of 52 distinct company locations providing contract distillation or purification services were identified. Of these, 32 were assessed to be capable or potentially capable of being used to purify CW-related, controlled chemicals above laboratory scale. Figure 5 displays the AG membership status of those locations. Once again, the majority of companies are located in AG member countries. Likewise, as shown in Figure 6, all are located in countries that either fully or partially incorporate the AG CCL of CW Precursors into their regulations. However, as previously noted, India and China impose STCs on all CWC scheduled chemicals, such that only purified chemicals listed by the AG but not the CWC potentially would fall outside of control.

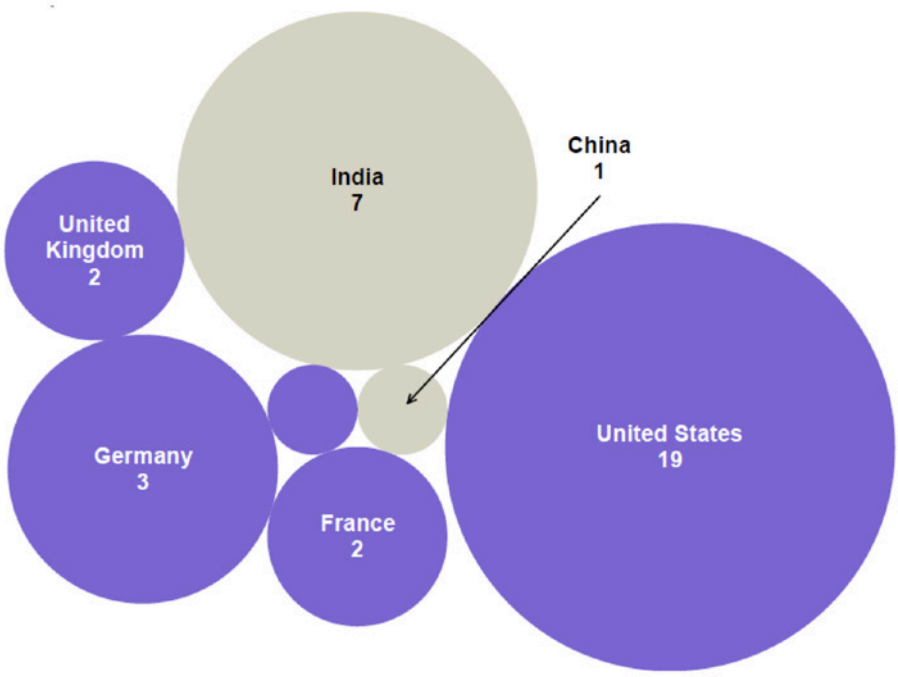

Figure 5. Number of companies offering CW-relevant distillation and purification services, grouped by location and AG membership status. Circle diameter qualitatively represents the count of distinct company names in each location. AG members are indicated by purple, with non-members in gray. A complete listing of locations and number of resident companies may be found in the Appendix (Table A5).

Figure 6. Number of companies offering CW-relevant distillation and purification services, grouped by location and adherence to the AG CW precursor control list. Rectangle size represents the count of distinct company names in each country. Full adherence is indicated in purple. Partial adherence is indicated in gray. A complete listing of locations and number of resident companies is provided in the Appendix (Table A6).

Biological Contract Services

Contract services of concern for potential BW production and related to STCs include fermentation (cultivation) of pathogens and toxins that would be subject to STCs. Further, contract lyophilization or other stabilization services such as spray drying are also of interest. Both of these are rate-limiting steps in the BW production process. Therefore, a survey was conducted of companies offering contract fermentation and contract stabilization services.

Fermentation Services

An investigation was conducted of providers offering contract fermentation services for both microbial and mammalian cells. These services are relevant for the cultivation of pathogens (viruses, bacteria, and fungi) and production of toxins listed on the AG CCL of Human and Animal Pathogens and Toxins and the AG CCL of Plant Pathogens.[21,22] A proliferator's inability to access fermentation expertise and equipment can serve as a chokepoint in the high quantity and high quality production of BW agents. Listed bacteria and fungi can be cultivated directly, while listed viruses are produced by cultivating mammalian host cells infected with the virus.

---

21 The Australia Group, "List of Human and Animal Pathogens and Toxins for Export Control," 2015, <http://www.australiagroup.net/en/human_animal_pathogens.html>.

22 The Australia Group, "List of Plant Pathogens for Export Control," 2012, <http://www.australiagroup.net/en/plants.html>.

Several AG-listed toxins can be produced by cultivating the toxin-producing microbial or mammalian producer cells.[23] The same database of custom manufacturers used for chemical contract service searches was queried for companies providing contract fermentation services.[24] This information was supplemented with companies listed as providing contract fermentation services from an independent database in a 2015 pharmaceutical contract manufacturing industry report.[25] The website of each company was reviewed to assess the company's ability to provide contract fermentation services, the types of cells they could cultivate, and the company's approximate total fermentation capacity.

Companies whose websites clearly indicated that they only fermented food products (e.g., beer, wine, cheese, and yogurt) were eliminated, but all other companies were included in analyses irrespective of their ability to provide biological containment required for safe handling of most AG-listed pathogens (Biosafety Level 3 [BSL3] or Biosafety Level 4 [BSL4]). The data were considered this way for two reasons. First, there are at least 32 AG-listed pathogens that are harmful to animals or plants, but are not harmful to humans. Second, several AG-listed toxins are proteins which can be expressed in cultured microbial or mammalian cells that do not normally produce toxins. Given limitations in available data, delving into issues of compliance and biosafety protocols for individual companies is beyond the scope of this paper. Of 123 contract fermentation company locations thus identified, two companies explicitly mentioned their "containment facilities," two additional companies referenced their ability to cultivate "infectious diseases," and a further two companies specifically mentioned their BSL3 biocontainment capabilities. All six companies were located in AG member countries.

Figure 7 displays the number of locations offering contract fermentation services, grouped by AG membership status. Similarly to the chemical contract services analyses, the majority of companies are located in AG member countries (104 of 123 companies, or 84%), with the exception of India, China, and Taiwan (19 companies). Further, as shown in Figure 8, all companies are located in countries or jurisdictions that either fully or partially adhered to the AG CCL of Human and Animal Pathogens and Toxins and the AG CCL of Plant Pathogens at the time of research conducted for this article. The Indian national control list and the Chinese national control list contained roughly 75% of the pathogens and toxins on the AG CCLs as of October 2016. Similarly to the chemical services analysis, adoption of an EU-style dual-use list or a national list matching the AG CCL of Human and Animal Pathogens and Toxins and the AG CCL of Plant Pathogens as of 2014 were considered as proxies for adherence to the list.[26]

---

23 Contract providers of peptide synthesis were not considered because the majority of AG-listed toxins are large, complex macromolecules and likely outside the present capability of such a contract service provider.

24 "Contract MFG," Chemical Information Services, <https://chemicalinfo.com/services/contractmfg/>.

25 *Contract Manufacturing in Pharmaceutical Industry, 2015-2025* (Vancouver: Roots Analysis, 2015).

26 This includes an assumption that these countries or jurisdictions will, at a legislatively appropriate time, update their control lists to reflect changes made by the EU or the AG—including the addition of severe acute respiratory syndrome-related coronavirus (SARS-related coronavirus) and reconstructed 1918 influenza virus as well as approximately 25 nomenclature changes since 2014.

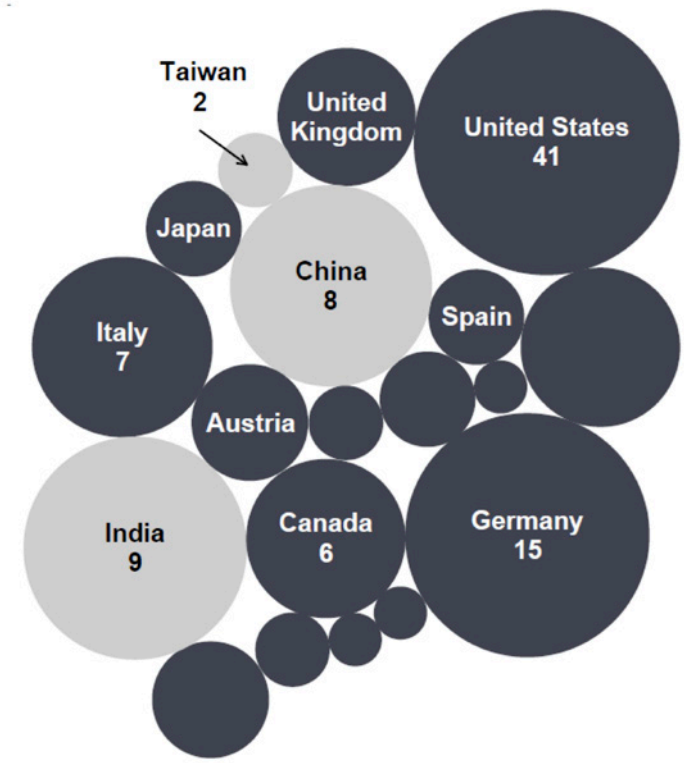

Figure 7. Number of companies offering BW-relevant fermentation services, grouped by location and AG membership status. Circle diameter qualitatively represents the count of distinct company names in each location. AG members are indicated by black, with non-members in gray. A complete listing of locations and number of resident companies may be found in the Appendix (Table A7).

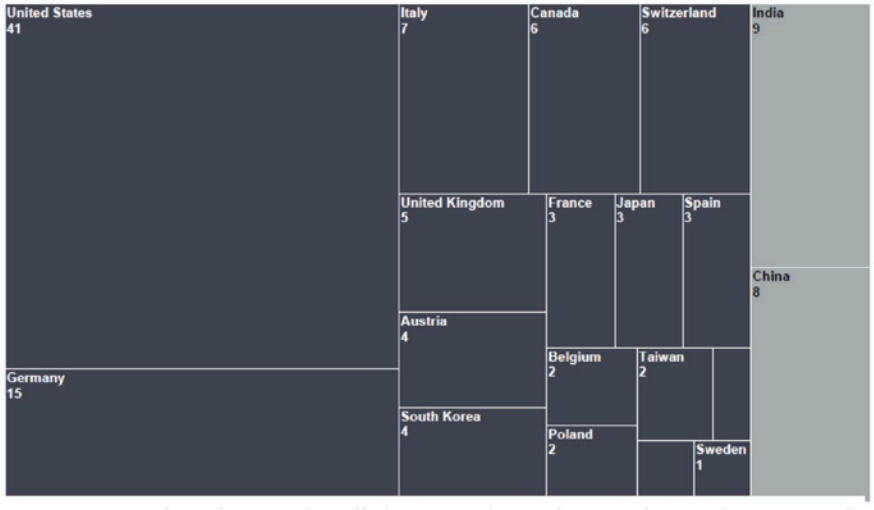

Figure 8. Number of companies offering BW-relevant fermentation services, grouped by location and adherence to the AG BW pathogens and toxins control lists. Rectangle size represents the count of distinct company names in each location. Full adherence is indicated in black. Partial adherence is indicated in gray. A complete listing of locations and number of resident companies is provided in the Appendix (Table A8).

Table 2 and Table 3 further break down the cell cultivation services offered by each identified company location, grouped by AG member status. While information provided on company websites varied, companies in both AG member and non-member countries/jurisdictions indicated their ability to cultivate bacteria, yeast, and mammalian cells. Table 4 displays the approximate cultivation capacity offered by each identified company location, grouped by AG member status. The majority of companies identified offered fermentation scales of between 101 and 10,000 L. All companies identified as a result of this analysis are likely to possess fermenters with cultivation capacities greater than the AG threshold for control (20 L), but delving deeper into specific company equipment holdings or service offerings was beyond the scope of this analysis.

AG Member	Location	Yes	Not provided
Yes	Austria	3	1
	Belgium	2	
	Canada	4	1
	France	2	1
	Germany	7	7
	Italy	4	3
	Japan	2	1
	Mexico	1	
	Netherlands		1
	Poland	1	1
	South Korea	1	3
	Spain	1	2
	Sweden		1
	Switzerland	3	3
	United Kingdom	1	4
	United States	20	21
No	China	1	7
	India	2	7
	Taiwan	1	1

Table 2. Number of companies offering BW-relevant fermentation services, grouped by AG membership status, location, and companies' stated ability to cultivate microbial (bacterial and yeast) cells. "Yes" indicates that the company provided this information on its website. "Not provided" indicates that the company provided no information on its website.

AG Member	Location	Yes	Not provided
Yes	Austria	2	2
	Belgium	1	1
	Canada	1	4
	France	3	
	Germany	8	6
	Italy	1	6
	Japan	2	1
	Mexico	1	
	Netherlands		1
	Poland	1	1
	South Korea	3	1
	Spain	2	1
	Sweden		1
	Switzerland	4	2
	United Kingdom	2	3
	United States	33	8
No	China	4	4
	India	1	8
	Taiwan	2	

Table 3. Number of companies offering BW-relevant fermentation services, grouped by AG membership status, location, and companies' stated ability to cultivate mammalian cells. "Yes" indicates the company provided this information on its website. "Not provided" indicates that the company provided no information on its website.

AG Member	Location	1-100	101-1000	1001-10,000	>10,001	Not provided
Yes	Austria	1		2	1	
	Belgium		2			
	Canada			1	3	2
	France	1	1	1		
	Germany	1	5	3	2	4
	Italy				1	6
	Japan			2		1
	Mexico				1	
	Netherlands					1
	Poland		1			1
	South Korea		1	1	1	1
	Spain		1	1		1
	Sweden					1
	Switzerland		1	2	2	1
	United Kingdom			2	1	2
	United States	4	13	9	7	11
No	China		2	1	1	4
	India		1			8
	Taiwan			1	1	

Table 4. Number of companies offering BW-relevant fermentation services, grouped by AG membership status, location, and the maximum fermentation capacity (in liters) provided by individual companies. "Not provided" indicates that the company provided no information on its website.

Stabilization Services

Companies offering contract lyophilization (freeze-drying) or spray-drying services were also investigated. These services are relevant for the preservation of pathogens and toxins listed on the AG CCL of Human and Animal Pathogens and Toxins and the AG CCL of Plant Pathogens. Preservation or stabilization is a critical step for a proliferator. Incorrect preservation of a pathogen or toxin likely results in its destruction shortly after production, but proper preservation means it can retain viability for weeks or months. The same databases used for identifying fermentation providers were queried for companies providing contract stabilization services. The website of each company was reviewed to assess the company's ability to provide contract stabilization services, whether it provided lyophilization or spray drying. On the basis of their target clients' general desire to produce large batches of pharmaceutical products, companies identified as providing contract stabilization services likely possess lyophilizers with condenser capacities of > 10 kg ice/24 hours and < 1000 kg ice/24 hours, which are the thresholds for control on the AG CCL of Dual-Use Biological Equipment.[27] The lyophilizers were also likely steam, gas or vapor sterilizable, given their repeated application in preservation of pharmaceutical products.

Figure 9 displays the AG membership status of 64 company locations identified as offering contract stabilization services. Similarly to all prior analyses, the vast majority of companies (56 of 64, or 87%) are located in AG member countries; the exceptions are India and China. Further, as shown in Figure 10, all companies are located in countries that either fully or partially adopt both the AG CCL of Human and Animal Pathogens and Toxins and the AG CCL of Plant Pathogens.

Figure 9. Number of companies offering BW-relevant stabilization services, grouped by country location and AG member status. Circle diameter qualitatively represents the count of distinct company names in each location. AG members are indicated by dark green, with non-members in light green. A complete listing of locations and number of resident companies may be found in the Appendix (Table A9).

27 The Australia Group, "Control List of Dual-use Biological Equipment and Related Technology and Software, 2015, <http://www.australiagroup.net/en/dual_biological.html>.

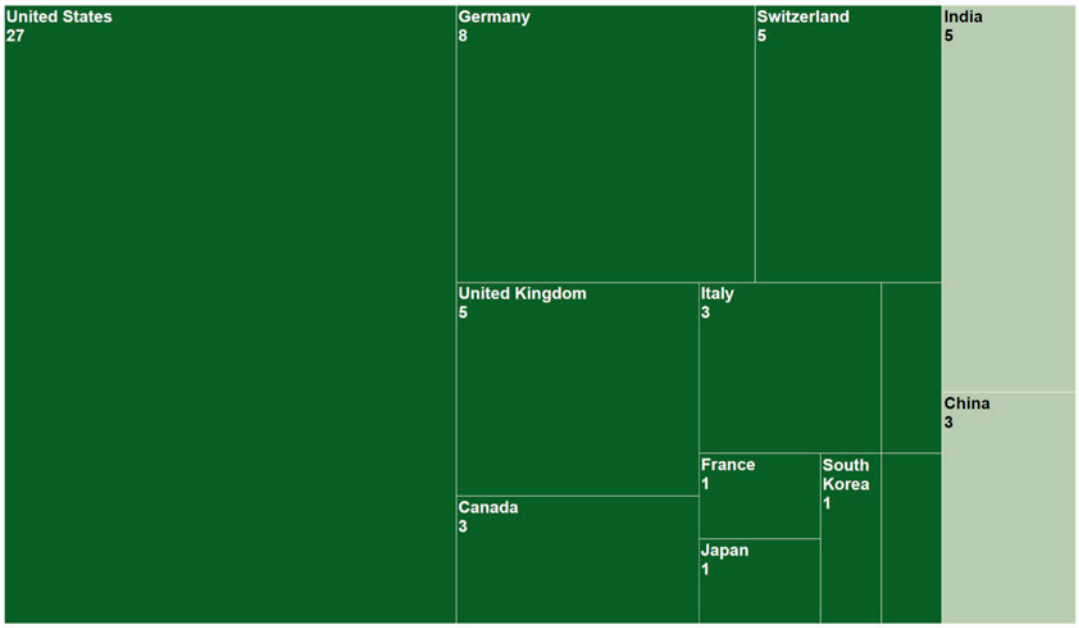

Figure 10. Number of companies offering BW-relevant stabilization services, grouped by location and adherence to the AG BW pathogens and toxins control lists. Rectangle size represents the count of distinct company names in each location. Full adherence is indicated by dark green. Partial adherence is indicated by light green. A complete listing of locations and number of resident companies may be found in the Appendix (Table A10).

Conclusion: Proliferation Potential of Contract Manufacturing and Implications for Strategic Trade Controls

The results of this survey indicate that there are hundreds of contract service providers potentially capable of synthesizing CWC Schedule 2 precursors that pose a significant proliferation risk. However, the vast majority of those companies are located in AG member countries or places where control lists include—in whole or in part—chemicals on the AG CCL of CW Precursors and integrate the CWC Schedules of Chemicals. In the case of contract distillation and purification service providers, this survey indicates that the vast majority of companies providing relevant or potentially relevant contract purification services are located in jurisdictions that have STC regulations in line with the AG and/or are CWC States Parties.

The survey of companies offering custom fermentation services found at least 123 worldwide locations providing this service, after excluding food producers. The survey of companies offering custom lyophilization or spray-drying services identified at least 64 worldwide locations engaged in this type of business with equipment that likely met AG specifications for control. While it is important to emphasize that this count is not exhaustive, analysis of these representative data in both cases indicates that a significant majority of companies identified are located in AG member countries or jurisdictions whose national control lists incorporate—in whole or in part—pathogens and toxins listed on both the AG CCL of Human and Animal Pathogens and Toxins and the AG CCL of Plant Pathogens.

These results indicate that most providers of dual-use chemical and biological contract services would be subject to laws and regulations that would prohibit contributing those services to CW or BW proliferant activities. Increasing company awareness of—and incentivization to comply with—existing STCs therefore becomes critically important for preventing the exploitation of these providers by proliferators. Although there is a sizable community of such companies, lack of literature on related outreach implies a need to engage them on STC compliance. Service providers of organophosphorus chemistry, fluorination, and fermentation could be prioritized as outreach targets based on the enhanced dual-use risk posed by those activities. Organizations tasked with such outreach to the chemical and biotechnology industries should ensure that contract service providers are not overlooked. Outreach efforts should focus on corporate due diligence, vetting of customers, and the internal compliance programs of the contract service provider.

Potential avenues for engagement include visits to individual contract service providers, contract manufacturing expos, related conferences, and professional organizations. Tools such as subscription-based databases of contract service providers could be utilized to identify outreach targets and ensure they are invited to outreach events. Increasing STC-related outreach to contract service providers and using this outreach to inform these companies about how they may be exploited will be especially important as advances in technology (e.g., synthetic biology) shift potential CW and BW concerns away from materials and commodities currently listed for export control and towards CW and BW concerns that are not listed and are increasingly harder to document on export control lists.

Appendix

AG Member	Location	
Yes	Austria	1
	Canada	8
	France	13
	Germany	17
	Hungary	2
	Italy	10
	Japan	11
	Mexico	3
	Netherlands	2
	Norway	2
	Poland	1
	Spain	2
	Sweden	1
	Switzerland	7
	United Kingdom	9
	United States	61
No	China	20
	India	26
	Israel	1
	Russia	2
	Taiwan	6
	Venezuela	1

Text

Table A1. Complete listing of locations and number of resident companies offering CW-relevant organophosphorus chemistries, grouped by location and AG membership status.

Adheres to AG Control Lists	Location	
Yes	Austria	1
	Canada	8
	France	13
	Germany	17
	Hungary	2
	Italy	10
	Japan	11
	Mexico	3
	Netherlands	2
	Norway	2
	Poland	1
	Russia	2
	Spain	2
	Sweden	1
	Switzerland	7
	Taiwan	6
	United Kingdom	9
	United States	61
Partial	China	20
	India	26
	Israel	1
No	Venezuela	1

Table A2. Complete listing of countries and number of resident companies offering CW-relevant organophosphorus chemistries, grouped by location and adherence to the AG CW precursor control list.

AG Member	Location	
Yes	Austria	3
	Belgium	6
	Canada	8
	France	20
	Germany	31
	Hungary	2
	Italy	27
	Japan	26
	Mexico	4
	Netherlands	2
	Norway	1
	Poland	5
	Portugal	1
	South Korea	2
	Spain	7
	Switzerland	15
	United Kingdom	25
	United States	111
No	China	64
	India	157
	Israel	3
	Taiwan	5
	Venezuela	1

Table A3. Complete listing of locations and number of resident companies offering chlorination and fluorination chemistries, grouped by location and AG membership status.

Adheres to AG Control Lists	Location	
Yes	Austria	3
	Belgium	6
	Canada	8
	France	20
	Germany	31
	Hungary	2
	Italy	27
	Japan	26
	Mexico	4
	Netherlands	2
	Norway	1
	Poland	5
	Portugal	1
	South Korea	2
	Spain	7
	Switzerland	15
	Taiwan	5
	United Kingdom	25
	United States	111
Partial	China	64
	India	157
	Israel	3
No	Venezuela	1

Table A4. Complete listing of countries and number of resident companies offering chlorination and/or fluorination reactions, grouped by location and adherence to the AG CW precursor control list.

AG Member	Location	Likely	Maybe	Unknown	Unlikely
Yes	Belgium		1		
	France	1	1		1
	Germany	2	1		2
	Switzerland				2
	United Kingdom	2	1		1
	United States	8	11		7
No	China			1	2
	India	2	3	2	1
	Venezuela				1

Table A5. Complete listing of countries and number of resident companies offering CW-relevant distillation and purification services, grouped by location and AG membership status. "Unknown" and "Unlikely" were not included in Figure 5.

Adheres to AG Control Lists	Location	Likely	Maybe	Unknown	Unlikely
Yes	Belgium		1		
	France	1	1		1
	Germany	2	1		2
	Switzerland				2
	United Kingdom	2	1		1
	United States	8	11		7
Partial	China			1	2
	India	2	3	2	1
No	Venezuela				1

Table A6. Complete listing of countries and number of resident companies offering CW-relevant distillation and purification services, grouped by location and adherence to the AG CW precursor control list. "Unknown" and "Unlikely" were not included in Figure 6.

AG Member	Location	
Yes	Austria	4
	Belgium	2
	Canada	6
	France	3
	Germany	15
	Italy	7
	Japan	3
	Mexico	1
	Netherlands	1
	Poland	2
	South Korea	4
	Spain	3
	Sweden	1
	Switzerland	6
	United Kingdom	5
	United States	41
No	China	8
	India	9
	Taiwan	2

Table A7. Complete listing of countries and number of resident companies offering BW-relevant fermentation services, grouped by location and AG membership status.

Adheres to AG Control Lists	Location	
Yes	Austria	4
	Belgium	2
	Canada	6
	France	3
	Germany	15
	Italy	7
	Japan	3
	Mexico	1
	Netherlands	1
	Poland	2
	South Korea	4
	Spain	3
	Sweden	1
	Switzerland	6
	Taiwan	2
	United Kingdom	5
	United States	41
Partial	China	8
	India	9

Table A8. Complete listing of countries and number of resident companies offering BW-relevant fermentation services, grouped by location and adherence to the AG BW pathogens and toxins control lists.

AG Member	Location	
Yes	Austria	1
	Canada	3
	France	1
	Germany	8
	Italy	3
	Japan	1
	South Korea	1
	Sweden	1
	Switzerland	5
	United Kingdom	5
	United States	27
No	China	3
	India	5

Table A9. Complete listing of countries and number of resident companies offering BW-relevant stabilization services, grouped by location and AG member status.

Adheres to AG Control Lists	Location	
Yes	Austria	1
	Canada	3
	France	1
	Germany	8
	Italy	3
	Japan	1
	South Korea	1
	Sweden	1
	Switzerland	5
	United Kingdom	5
	United States	27
Partial	China	3
	India	5

Table A10. Complete listing of countries and number of resident companies offering BW-relevant stabilization services, grouped by location and adherence to the AG BW pathogens and toxins control lists.

Dual-use Research and Trade Controls: Opportunities and Controversies

CHRISTOS CHARATSIS[1]

Abstract

This article intends to clarify the role of trade controls in relation to dual-use research, stimulate the debate on the possible contribution of trade controls to the broader governance of sensitive research, and inspire ways to achieve this in practice. First, the article discusses the different interpretations of the term dual-use research by highlighting its relevance in the context of nonproliferation, research ethics and the dual-use industry. The article offers a working definition for export controlled research activities. Second, the article explores why there is a nexus between trade controls and research. In this regard, the added value and known shortcomings connected to trade control implementation is presented. The article discusses the European and American experience in implementing trade controls to research activities. In addition, the paper attempts a first assessment of the new elements affecting research as set forward by the recent European Commission (EC) proposal for the review of the dual-use regulation. Finally, the article presents a typology of measures presently governing dual-use research while highlighting their synergetic value when applied in combination with trade controls.

Keywords

Dual-use research, export controlled research, biosecurity, research ethics, technology transfers, EU export control policy review, tacit knowledge, fundamental research, disruptive technologies

1 Christos Charatsis is a multidisciplinary practitioner with academic and public sector experience in strategic trade controls and international security. He holds a doctoral diploma in Political Science from the University of Liege with a focus on the implications of export controls law for research organizations. He presently works as a project officer at the European Commission Joint Research Centre providing support to the EU Partner-to-Partner Export Control Program and conducting research on a variety of strategic trade control issues such as the implementation of the Regulation 428/2009, dual-use research and internal compliance.

Introduction: The Duality of Knowledge and WMD Proliferation

While almost every technology can be misapplied if one has the intention to do so, there are some types of technology that are considered particularly sensitive due to their "dual" usefulness. Concurrently, the proliferation of Weapons of Mass Destruction (WMD) still represents a problem threatening humanity with complete obliteration. As Smith neatly mentions, the nature of the […] proliferation problem confronting mankind is, in its fundamental sense, a "problem" of knowledge.[2] For instance, in the past, nuclear proliferation took place through effective espionage, deliberate transfer of technology to allied countries and scientists changing ideological camps. Indeed, Reed and Stillman argue that the acquisition of Western nuclear technology by China did not rely primarily on espionage but was accomplished one graduate student at a time.[3] Therefore, it may not be an exaggeration to claim that the dual-use problem finds in WMD proliferation its most glaring manifestation.

Technology is defined as the practical application of knowledge to the practical needs of society and strategic trade controls aim at addressing the dual-use problem by providing a system for monitoring transfers of tangible materials and items as well as intangible transfers of technology and software.[4] As a result, research activities and trade controls intersect. However, the dual-use problem has broader security and ethical implications and may concern a broad range of activities and types of research not necessarily interrelated to activities and technologies targeted by trade controls.

After the nuclear trend, life sciences have been in the spotlight for several years partly due to unprecedented innovations (e.g., synthetic genomics) achieved in that area and incidents suggesting the existence of new security threats (e.g., the 2001 anthrax mail attacks). In relation to this, the body of literature dedicated to risks stemming from emerging technologies in biological and chemical field have influenced the author's ideas in mapping out and understanding the issues involved in the so-called "research of dual-use concern." Tucker, in particular, argues that different types of technologies warrant specific governance measures and goes far enough to define a methodology for identifying the right mix of measures (hard-law, soft-law, and informal measures) for any given emerging bio-technology.[5] In his significant work he also highlights that the weaponization of nuclear, biological, and chemical materials and equipment is a technically challenging process involving both explicit and tacit knowledge. In particular, knowledge as it is expressed in its tacit form—skills, know-how, and sensory cues that transferred mainly through personal contacts—is a key capability not always diffused or readily available.

---

2 Roger K. Smith, "Explaining the Nonproliferation Regime: Anomalies for Contemporary International Relations Theory," *International Organization* 41 (1987), p. 266.

3 Thomas C. Reed and Danny B. Stillman, *The Nuclear Express: A Political History of the Bomb and its Proliferation,* (Minneapolis: Zenith Press, 2009), p. 87.

4 Definition inspired by the common definitions used in dictionaries. Check for instance, the definition in the Merriam-Webster Dictionary, available in: <https://www.merriam-webster.com/dictionary/technology?utm_campaign=sd&utm_medium=serp&utm_source=jsonld>.

5 Jonathan B. Tucker, *Innovation, Dual-use, and Security, Managing the Risks of Emerging Biological and Chemical Technologies* (Cambridge: The MIT Press, 2012), see in particular chapters 4 and 21.

In spite of this, nowadays tacit knowledge is becoming increasingly available due to the global distribution of skilled staff and the extensive collaboration between industry and academia in the research and development (R&D) phase. As Meier highlights, globalization leads to technology diffusion and it is inexorably linked to the sharing of technologies, including dual-use technologies.[6] In this context, the role of key stakeholders—industry and academia—are of central importance in achieving security imperatives including trade controls objectives.

At a time when a new generation of disruptive technologies (e.g., artificial intelligence, 3-D printing, cloud computing, synthetic genomics) are already being widely used and the WMD term is stretching to accommodate less destructive weapons such as radiological dispersal devices, explosives, and cyber weapons, the article intends to:

- Clarify what dual-use research is;
- Define export controlled research;
- Explain the role of trade controls in this broader context and,
- Identify the typology of other available mechanisms for overseeing dual-use research.[7]

Conceptualizing Dual-use Research

The term dual-use research is composed of two elements: research and dual-use. Research can be defined as "investigation or experimentation aimed at the discovery and interpretation of facts, revision of accepted theories or laws in the light of new facts, or practical application of such new or revised theories or laws."[8] Dual-use is generally understood as anything having more than one use and most frequently, as any item that can be used for both benevolent and malign purposes. These basic definitions provide the impetus for making two reflective observations on the understanding of dual-use research and the main dimensions of the problem.

First, considering the definition of research as cited above, the term may include all the different activities potentially involved in research, from the observation of main principles, conduct of analytic studies and experiments, and testing of proof-of-concepts, to the building of prototypes and the actual application of such models to the needs of society at the industrial level through additional modifications. In this view, the term covers both industry and academic research and

---

6 Oliver Meier, *Technology Transfers and Nonproliferation of Weapons of Mass Destruction: Between Control and Cooperation* (Oxon: Routledge, 2014), p. 9.

7 For instance on the relationship between the WMD term and cyber security see: Clay Wilson, "Cybersecurity and Cyber Weapons: Is Nonproliferation Possible?," in Maurizio Martellini, *Cyber Security Deterrence and IT Protection for Critical Infrastructures* (Springer Briefs in Computer Science, 2013), p. 17.

8 See the online Merriam-Webster Dictionary, <http://www.merriam-webster.com/dictionary/research>.

links closely with another broadly used term – research and development (R&D).[9] Second, the dual-use concept is quite broad and thus can accommodate varying understandings.

The first observation implies that one could intervene in different phases of a research project in order to examine possible security implications. For instance, a scientist could envision the benefits and risks of research already in the phase of inception so as to take any necessary precautions. University institutions or government authorities could evaluate any possible risks relating to a research proposal and design mitigating measures from the very beginning. One should, however, consider that the potential of research to produce an outcome of dual-use concern may become evident only during the lifetime of the research or even at the end. As a result, the right avenue for overseeing dual-use research may vary depending on the phase of a project and the nature of research per se.

Concerning dual-use, some confusion exists due to various understandings of the term by different professional communities or even among practitioners of one single community. More specifically, the term dual-use research is encountered mainly in three different contexts:

- Nonproliferation and strategic trade controls area;
- Research ethics discourse (chiefly in life sciences) and,
- Synergies between the military/defense and civil organizations.

First, in the nonproliferation purview, dual-use research is not often used as such yet it is implied. For example, the US Export Administration Regulations use the term research and so does the EU dual-use regulation when referring to the "basic scientific research exemption" setting fundamental research out of the scope of trade controls.[10] In practice, the EU system follows the example of Multilateral Export Control Regimes (MECRs) by simply incorporating the decontrol notes of basic research and public domain information without further clarifying the intersection of trade controls with research activities. However, this absence of dual-use research from European and international law does not imply a lack of interest on the topic itself.[11]

---

9 "Research and experimental Development (R&D) comprise creative work undertaken on a systematic basis in order to increase the stock of knowledge, including knowledge of man, culture and society, and the use of this stock of knowledge to devise new applications" as defined in *Frascati Manual: Proposed Standard Practice for Surveys on Research and Experimental Development* (Paris: OECD, 2002), p. 30, <http://www.oecd.org/sti/inno/frascatimanualproposedstandardpracticeforsurveysonresearchandexperimentaldevelopment6thedition.htm>.

10 Title 15 CFR, Part 734 §8 of the US EAR and the Nuclear Technology Note of Council Regulation (EC) No. 428/2009 of 5 May 2009, Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items, Official Journal of the European Union (L 134/1) of May 29, 2009.

11 The author has conducted doctoral research on the interferences between export controls and dual-use research for the University of Liège and on behalf of the European Commission Joint Research Centre. Additionally, several seminars and EU meetings have discussed this topic. Indicatively: *55th Dual-Use Coordination Group*, September 25, 2015, Brussels; "King's College Event on Intangible Technology Controls in Industry and Academia, March 29, 2016, London <http://iipdigital.usembassy.gov/st/english/publication/2008/08/20080815121848xjyrrep0.1191522.html#>; Joint JRC-NNSA Technical Seminar/ 6th ESARDA Export Control Working Group, April 22-23, 2015, Ispra, Italy.

Dual-use research has entered the spotlight for a number of reasons and this is reflected more frequently in formal yet not legally binding texts. For instance, the European Commission (EC) Communication for the review of the EU export control system notes the imperative "to clarify the control of dual-use research while avoiding undue obstacles to the free flow of knowledge and the global competitiveness of EU science and technology."[12] It also acknowledges the need for "targeted and coordinated outreach for academic research communities throughout the EU."[13] In the same refrain, the recent EC proposal for the recast of the regulation refers explicitly to the relationship of research with trade controls in three instances: the definition of exporter, the new general license for intra-company transmission of software and technology, and the imperative not to prevent the export of information and communication technology used for legitimate purposes, including law enforcement and internet security research.[14]

In an international context, in 2016, the United Nations Security Council resolution 1540 Civil Society Forum took place with the aim of providing an opportunity for academia and civil society to contribute to the work of 1540 Committee in the context of the resolution's comprehensive review. The report, presenting the outcomes of discussions, highlights a host of measures for engaging academics in different aspects of the implementation of the resolution including tackling dual-use research especially in the life sciences.[15]

Second, in research ethics discourse, the dual-use concept appears to comprise any type of research that can be misused. At a practical level this became particularly evident in the preparation of a guidance document by EC with the aim to educate researchers submitting proposals in the framework of Horizon 2020 on identifying any dual-use issues relating to their research.[16] The exchanges between security experts and ethics reviewers showcased how broad the dual-use concept may be. The term concerns in principle research having both civil and military applications. Additionally, it can accommodate a variety of research types such as vulnerability studies uncovering details on critical infrastructure, research projects developing software applications that could be misused, or research on new psychotropic substances that can be used for both medical purposes and as alternatives to controlled substances. In that

12 European Commission, "Communication for the Commission to the Council and the European Parliament: The Review of Export Control Policy: Ensuring Security and Competitiveness in a Changing World," COM(2014)244 final, <http://trade.ec.europa.eu/doclib/docs/2014/april/tradoc_152446.pdf>, p. 7.

13 Ibid.

14 EU Commission, "Proposal for a Regulation of the European Parliament and of the Council Setting Up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (recast)," COM(2016) 616 final, Brussels, 2016, <http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154976.pdf>.

15 "UNSCR 1540 Civil Society Forum: A Dialogue with Academia and Civil Society Meeting Report," United Nations University Centre for Policy Research, June 2016, <https://i.unu.edu/media/cpr.unu.edu/attachment/2187/Meeting-Report-UNSCR-1540-Civil-Society-Forum.pdf>.

16 The result of this consultation was a "Guidance Note for Research Involving Dual-Use Items" aimed at facilitating the ethics self-assessment review required from H2020 applicants, available in: <http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-dual-use_en.pdf>.

view, Rath et al. note a lack of a universal understanding of dual-use research in the literature pertaining to ethical discourse.[17]

Nevertheless, there is an area of research ethics where dual-use research is specifically defined. Dual-use research in bio-science is considered an area of particular concern since "almost all biotechnology in service of human health can be subverted for misuse by hostile individual or nations."[18] Indeed, scholars in this area refer often to dual-use research of concern (DURC), a term specifically coined to describe sensitive dual-use research in life sciences and used primarily by organizations such as the World Health Organization (WHO) and the American National Science Advisory Board for Biosecurity (NSABB).[19] The legal dispute over the Dutch licensing authority asking for an export authorization for the publication in a well-known journal of a research study exploring the transmissibility of H5N1 virus between mammals turned in part the attention to the possible connections between trade controls and bio-related research.[20]

The third occurrence of dual-use research resides in the interactions between military/defense and civil organizations. From this perspective, the term is used to describe technologies and items that originate from either military or civilian organizations and can have applications in whichever area. As Gallart mentions, "historically there is a shift of focus from R&D outputs derived from military industry and applied for civilian purposes (spin-off) to technological developments occurring elsewhere in the economy and exploited for the benefit of military production (spin-in)."[21] As a result, policymakers at the European and EU Member State level who are not directly concerned by proliferation objectives perceive dual-use research as an opportunity for reinforcing innovation and strengthening the combined output of industry through the development of synergies between defense and civil firms. The EC has taken several initiatives for bolstering the European defense sector, such as incentivizing public authorities and the private sector to invest more in the potential of dual-use research.[22]

---

17 Johannes Rath, Monique Ischi and Dana Perkins, "Evolution of Different Dual-Use Concepts in International and National Law and its Implications on Research Ethics and Governance," *Science and Engineering Ethics* 20:3 (September 2014), p. 770.

18 "Biotechnology Research in an Age of Terrorism (The Fink Report)," National Research Council, Washington, DC, The National Academy Press, 2004, preface.

19 Dual-use research of concern (DURC) is life sciences research that is intended for benefit, but which might easily be misapplied to do harm, retrieved from the WHO website: <http://www.who.int/csr/durc/en/>. See also the complete definition from the US National Institute of Health, available in: <http://osp.od.nih.gov/office-biotechnology-activities/biosecurity/dual-use-research-concern>.

20 Robert Shaw, "Export Controls and the Life Sciences: Controversy or Opportunity?," Volume 17, *EMBO Reports* 17:4, (2016), pp. 474–480; Angela Cirigliano et al., "Biological Dual-Use Research and Synthetic Biology of Yeast," Science and Engineer Ethics 23:3 (June 2016), pp. 1-10; Christos Charatsis, "Setting the Publication of 'Dual-use Research' under the Export Authorization Process," *Strategic Trade Review* 1:1 (Autumn 2015), pp. 56-72.

21 Jordi Molas-Gallart, "The Political and Economic Context of European Defense R&D," *University of Sussex Electronic Working Papers Series* 52 (2000), p. 2.

22 See for instance: European Union, "Communication Towards a More Competitive and Efficient Defense and Security Sector," COM (2013) 542 final, Brussels, 2013, <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52013DC0542>; European Commission, "EU Funding for Dual-use: A Practical Guide to Accessing EU Funds for European Regional Authorities and SMEs," October 2014, <http://s3platform.jrc.ec.europa.eu/-/eu-funding-for-dual-use-guide-for-regions-and-smes?inheritRedirect=true>.

To circle back to trade controls and nonproliferation, trade controls may link to certain types of dual-use research as understood in the different contexts pinpointed above. However, dual-use trade controls, as largely list based instruments, cover only certain dual-use technologies falling within the defined thresholds and having specific performance capabilities. The fact that the trade control community lacks a commonly agreed definition of what dual-use goods mean adds complication to an already complex picture.[23] Therefore, it might be useful to offer a working definition of dual-use research, or to be more accurate, of 'export controlled research:

> *Export controlled research is defined as those research and development activities involving items, technologies, and software restricted under relevant trade control law. It concerns primarily civil research activities that are considered as integral to the design, construction, use, and delivery of Weapons of Mass Destruction and in some instances of conventional weapons.*[24]

This definition serves a number of purposes:

1. It refers solely to those research activities falling within the scope of trade control law but not to all research of dual-use nature. It is only the export of certain items and technologies that requires an authorization and may result in legal sanctions for the violators. The term R&D indicates that both basic and applied research may be in the scope of controls, if they involve controlled items.

2. The dual-use goods definitions adopted in the framework of MECRs point to an element of a major contribution for the development of military capabilities.[25] The definition denotes this element with the use of the adjective "integral."

3. It clarifies that the scope of trade controls concerning tangible items (materials, equipment, components, etc.) as well as technology (technical data and technical assistance) and software.

4. Dual-use research may be associated with technologies and items capable of contributing to the development of both WMD and conventional weapons. In line with the spirit of the law and the contents of dual-use control lists, the definition covers also conventional weapons and related end-uses.

---

23 For example, Quentin Michel and Andrea Viski have highlighted this problem in "Dual-Use: An Undefined Term?," Presentation prepared for the 3rd ESARDA Export Control Working Group, November 13, 2013, Ispra, Italy.

24 The definition derives from the doctoral study: C. Charatsis, "Interferences between Nonproliferation and Science: 'Exporting' Dual-Use Know-How and Technology in Conformity with Security Imperatives," University of Liege (forthcoming).

25 The NSG for instance, connects dual-use items to "certain equipment, materials, software and related technology that could make **a major contribution** to 'a nuclear explosive activity', an 'unsafeguarded nuclear fuel cycle' or 'acts of nuclear terrorism' without defining further the term. The WA provides that "dual-use goods and technologies to be controlled are those which are **major or key elements** for the indigenous development, production, use or enhancement of military capabilities.

Overall the definition is inspired by the definition provided in United Nations Security Council resolution 1540. The resolution seems to imply reference to dual-use goods when it expresses concern over the illicit trafficking in nuclear, chemical, or biological weapons and their means of delivery, and related materials. Indeed, in a footnote, it is clarified what "related materials" shall mean:

> *"Materials, equipment and technology covered by relevant multilateral treaties and arrangements, or included on national control lists, which could be used for the design, development, production or use of nuclear, chemical, and biological weapons and their means of delivery."*[26]

The Nexus between Trade Controls and Dual-use Research

The term dual-use applies to situations where a dual-use dilemma arises. For instance, to what extent can research having a peaceful or even a life-saving application be misused? Further, how could a researcher share blueprints, source codes, and know-how of innovative dual-use technologies without undermining security objectives? Dual-use trade controls offer—maybe unintentionally—some leverage for addressing this dilemma. The analysis below discusses the linkages between trade controls and research by highlighting the merits and drawbacks of the former for the latter.

Why is there a Nexus?

Trade controls were not designed as a tool for the governance of dual-use research. Indeed, the term until recently was hardly used in formal or legally binding texts. In alignment with this, decontrol notes, crafted in the framework of the MECRs, exclude fundamental research and information falling in the public domain from the scope of controls. That said, researchers still have a responsibility for applying for an export authorization when they export tangible dual-use items and materials in the framework of their research. Such activities are not negligible.[27] Additionally, the scope of controls extends to transfers of technology (technical data and assistance) and software including transfers through electronic means, the so-called 'intangible' ones. With this in mind, common activities undertaken in the framework of research such as posting software codes, sharing diagrams and technical information through emails or providing technical services abroad fall within the scope of controls if certain conditions apply.[28] Increasing collaboration between universities and firms and the related changing nature of academic research, moving steadfastly towards applied applications, make export control screening all the more necessary.

Interestingly, the scope of controls has been expanding to cover not only different types of activities (technology transfers, transit, and brokering) but also to accommodate new technologies by adjusting control lists so as to keep pace with new technological advancements.

---

26 United Nations Security Council 1540, S/RES/1540, New York, April 2004.

27 Discussion with US official in the margins of the 9th JRC-NNSA Technical Seminar, Ispra, Italy, June 16-17, 2016.

28 Christos Charatsis, "Setting the Publication of 'Dual-use Research' under the Export Authorization Process," *Strategic Trade Review* 1:1 (Autumn 2015), pp. 57-58.

One could glean some striking examples showing the sometimes proactive role of trade controls. The Wassenaar Arrangement (WA) dual-use list maintains controls concerning information security technologies and software. In 2013, the WA agreed upon the introduction of additional controls on technologies relating to intrusion software. In the cyber security arena, the recent EC proposal sets forward the unilateral implementation of controls on certain types of cyber surveillance technologies. Concurrently, different international regimes and the EC examine the usefulness of including in the scope of controls on equipment and technology relating to the manufacture of 3-D printers.[29]

The Importance of Including Trade Controls in the Mix of Dual-use Research Governance

There are several further factors to consider when contemplating the fitness and readiness of trade controls to address dual-use research concerns. These are listed here:

- The nature of controls has been shifting from a system of denial of technology to a system of monitoring. Only a limited number of transactions are prohibited as well as the number of denied export authorizations.
- Trade controls represent rather agile frameworks. Their flexibility consists in the fact that their main principles and control lists are negotiated and regularly updated in the framework of MECRs. They also provide a possibility for the application of ad hoc controls and prohibitions in the event of a transaction involving sensitive end-uses or end-destinations (e.g., embargoed and sanctioned countries or diversion hubs) and items with technical parameters close to the controlled ones.
- Trade controls envisage a number of trade facilitations such as general licenses in the EU and license exemptions in the US for compliant exporters operating from and exporting to less risky destinations.
- Trade controls offer exemptions for technology and software generally available to the public as well as for basic scientific research.
- Trade controls contribute to the development of standards for internal compliance for industry and academic organizations. Such standards when coupled with other safety and security rules (e.g., laboratory protocols and physical protection measures) can better guarantee the overall security of such organizations and instill a culture of compliance.

In relation to this last element, holding industry and universities accountable is important for one other reason. The center of innovation seems to be moving from defense to civil industry as "armed forces and defense industry's dependence on technologies with a civilian origin is increasing."[30] By extension, governments' control over commercial innovations—that are

29 For instance, the former NSG chair Ambassador Rafael Grossi confirmed in the EU Nonproliferation Conference (November 2016) that ongoing NSG discussions consider the implications of 3-D printing. At the EU level, the first discussion on this topic took place already in 2013.

30 European Commission, "EU Funding for Dual-use: A Practical Guide to Accessing EU Funds for European Regional Authorities and SMEs," October 2014, <http://s3platform.jrc.ec.europa.eu/-/eu-funding-for-dual-use-guide-for-regions-and-smes?inheritRedirect=true>, p.7.

potentially game changers for modern warfare—is limited compared to the oversight they exercise over defense related innovations. Trade controls as legally binding instruments function also as a pressure lever to firms and research institutes for researching and trading responsibly.

Drawbacks of Implementing Technology Trade Control Provisions

Trade controls are not a panacea for every type of technology considered to be dual-use. Trade controls seek to prevent the proliferation of most sensitive technologies relating to the construction of WMD, their means of delivery and certain military end-uses. In drafting their lists, trade controls regimes take into account certain criteria such as:[31]

a) Foreign availability outside the participating states;

b) Ability to effectively control the export of goods;

c) Ability to make a clear and objective specification of the item;

d) Whether the item is controlled by another regime.

Not all types of sensitive technologies are eligible to be covered by the dual-use lists. However, as explained above, the scope of controls can be adjusted based on new developments and perceptions of the most persistent risks and what the term WMD may include. The issue of foreign availability is also particularly important since it indicates technological areas where the implementation of controls is or has become meaningless due to the diffusion of a technology. At the same time, foreign availability hints at a need for universalizing trade controls by holding all suppliers of controlled technologies accountable.

More than a restrictive or discriminatory measure, trade controls function to deter, detect, delay, and prevent the diffusion of sensitive technologies. However, the present enforcement of technology controls is imperfect. In particular, the effectiveness of technology controls is fundamentally challenged by variance in national implementation.[32] The effectiveness of technology controls can be indirectly benefited by fostering transparency and accountability. In that regard, publishing licensing data concerning both tangible and intangible transfers and reporting on the systematic outreach activities and inspections conducted to industry and academia are steps to consider. States' asymmetrical implementation of controls by can harm their overall effectiveness since lax implementation in one country could lead to license shopping by unlawful state and non-state actors. Setting common standards where possible at the international level and increasing cooperation through exchange of information and best practices could improve the current situation. The 2006 "WA Best Practices for Implementing ITT Controls," underlining the role of industry, academia, and individuals in furthering compliance with technology controls represent only a first step in the right direction.[33]

---

31 See footnote in the WA document specifying the "Criteria for the Selection of Dual-use Items" available in: <http://www.wassenaar.org/controllists/2005/Criteria_as_updated_at_the_December_2005_PLM.pdf>.

32 Ian J. Stewart, "The Contribution of Intangible Technology Controls in Controlling the Spread of Strategic Technologies," *Strategic Trade Review* 1:1 (Autumn 2015), p. 54.

33 Wassenaar Arrangement, *Best Practices for Implementing Intangible Transfer of Technology Controls*, WA Plenary 2006, <http://www.wassenaar.org/wp-content/uploads/2015/06/ITT_Best_Practices_for_public_statement_2006.pdf>.

Trade controls, in addition, may be perceived as being at odds with the academic freedom and the imperative to protect the free circulation of information and the peaceful advancement of science. It is an inalienable right of researchers to perform their activities in an autonomous way and without unnecessary interference by any authority. This is a civil right enshrined in many countries also constitutionally.[34] Nonetheless, academic freedom is not unlimited either. "Academic freedom automatically includes academic responsibility, both for the university as a whole and for the individual professor or researcher."[35] In that view, section 8 §1 of the UK Export Act (2002) clarifies succinctly the role of trade control authority *vis-à-vis* cases raising questions on the protection of civil rights: "any interference of protected freedoms must be no more than is strictly necessary."[36] Another element to ensure is the existence of checks and balances keeping the authority accountable on its amplitude to require an export authorization for a research activity.

Addressing Dual-use Research Through Trade Controls: Current Approaches

Implementing trade controls in an academic context is particularly challenging. On the one hand, researchers, already faced with a number of ethics and integrity rules, safety and security regulations, and ensuing licenses and approvals, are required to take additional mitigating measures and produce extra paperwork for conducting research. On the other hand, authorities, often subject to spare resources and within the limits of available expertise, need to process license applications quickly, assess the risks stemming from complex research, conduct outreach activities, and inspect whether research organizations conform to existing obligations set in the law. The distinct mind-set encountered in academic environments hints at the intrinsic difficulties in communicating export control risks and imperatives to the academic and scientific community. For instance, an official from the US Department of Commerce (DOC) noted that the initial efforts of US authorities—about 15 years ago—to reach out to a university audience were unsuccessful.[37] Only when they contacted those higher in rank (deans, faculty presidents), were they effective in building bridges of understanding and communicating trade control objectives to scientific staff and students. Likewise, in Europe, Hungarian authorities were confronted with a similar attitude and a negative predisposition towards governmental controls of sensitive research during awareness raising seminars conducted in the past years in selected universities.[38]

---

34 For example, Article 5 §3 of the German basic law foresees that "arts and sciences, research and teaching shall be free." It is also noted though that "the freedom of teaching shall not release any person from allegiance to the constitution."

35 Andre Oosterlinck, "The Modern University and its Main Activities," in Luc E. Weber and James J. Duderstadt, *Reinventing the Research University* (France: Economica, 2004), p. 121.

36 United Kingdom Export Control Act, 2002, pp. 5-6, available in: <http://www.legislation.gov.uk/ukpga/2002/28/pdfs/ukpga_20020028_en.pdf>.

37 Discussion with the Director of Office of Nonproliferation and Treaty Compliance, A. Lopes, December 3, 2015.

38 Discussion with Director of the Hungarian licensing authority, September 24, 2015.

The State of Play in the European Union

Researchers and research organizations in the European Union experience varying approaches adopted by different Member States. An issue of central importance in implementing trade controls in the research context is the clarification of decontrol notes: What could be a working definition for "basic scientific research" in view of trade control law? How can software and information "falling in the public domain" be defined? The EU dual-use regulation does not clarify further the application of decontrol notes save the definitions provided in the framework of MECRs.[39] In the same line, most Member States have not adopted any national legislation or guidance on the nexus between trade controls with research.

Despite this, certain EU Member States have attempted to clarify how these exemptions shall work in practice.[40] For instance, as regards the publication of research deemed dual-use, the British and Dutch authorities consider that the process of making research available for publication abroad can be subject to authorization.[41] In practical terms, submitting a publication containing sensitive data or methodologies in a journal or a publishing house outside the EU could require an export authorization in the view of certain Member States. With this in mind, it is worth wondering whether any scientific papers—apart from the Fouchier work—have been requested to take an export authorization in any EU Member State. Concerning the public domain exemption some Member States such as the UK and Germany consider that when controlled items and technologies are to be bought from a supplier who controls the supply, or require registration or are restricted for access by certain people, then they do not pertain to the public domain.[42] When it comes to technology and software transfers, such general principles may need further clarifications and guidance. Concerning the enforcement of such controls, some Member States are known to have implemented both outreach activities and controls toward research organizations particularly those being active in nuclear and defense related research. For instance, in Germany, some of the most renowned research establishments conducting research of both basic and applied nature have taken specific internal measures as a result of such government communications and awareness raising seminars.[43]

---

39 Definitions used invariably by all MECRs: 'Basic scientific research' or 'fundamental' is experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective. 'In the public domain' means "technology" or "software" which has been made available without restrictions upon its further dissemination.

40 See for instance: UK Department of Business, Innovation and Skill (BIS), Export Control Organization, *Guidance on Export Control Legislation for Academics and Researchers in the UK*, 2010, available in: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/68680/Guidance_on_Export_Control_Legislation_for_academics_and_researchers_in_the_UK.pdf>.

41 Discussion with UK official in the King's College Event on Intangible Technology Controls in Industry and Academia, March 29, 2016.

42 UK BIS, *Guidance for Academics*, p. 8; Discussion with German official in the margins of the 42nd Dual-Use Coordination Group, pp. 23-24 October, 2013, Brussels.

43 The Helmholtz and the Fraunhofer Associations conduct research of mainly basic and applied character respectively and both have in place export compliance structures in the different establishments of their associations. Discussions and interviews with the export control officers from Helmholtz Association Berlin (HZB) and Fraunhofer, December 2015.

Thus far, the EU experience points to a non-compact and homogeneous approach. The insight of practitioners working in different parts of the R&D chain is enlightening. Compliance officers in certain research centers feel perplexed in deciding whether a publication is sensitive or whether sharing a source code requires an export authorization.[44] In addition, industry compliance officers confirm that export controls affect their collaboration with academia.[45] For example, technology transferred in the course of collaborative projects may be subject to an export authorization when research partners are located outside the country of establishment. To quote one of the officers, "We apply export controls *vis-à-vis* academic institutions in the same way as for other research partners."[46] Moreover, technology developed may be controlled and thus, subject to authorization. Information classified due to proprietary or security reasons warrants certain assurances and may require export authorizations as well. It might be also necessary for companies to ensure that their partners can only access those parts of their information systems that relate directly to the project in execution and/or for which an export authorization has been granted. Another practitioner noted that sometimes research institutes are not aware of trade control issues and researchers challenge the applicability of trade control provisions as pursued through non-disclosure agreements.

The Recast of the Regulation: An Opportunity?

The reform of the EU trade control system may represent an opportunity not to be missed. A long process of public consultation, initiated with the Commission's Green Paper from 2011, led to a proposal set forth by the EC for streamlining and modernizing the dual-use regulation. The proposal suggests, *inter alia*, the introduction of further EU general authorizations (e.g., intra-EU transfers, low-shipments, and large projects), the revision of terminology and previous ambiguous language (e.g., definitions of export, exporters, and transit) and the reform of the catch-all clause. The new text refers to research in recital five when discussing the imperative not to hinder internet security research. Also, recital eight emphasizes the need for a new definition of exporter captures all different categories of natural persons involved in the export of dual-use items including researchers and even a person downloading controlled technology.

Most interestingly, the revised language introduced for controls on intangible transfers of technology has de facto some bearing for research activities. Under the new definition of export and exporter the mere transmission of technology to a destination abroad is not any more controlled. However, in the case where the technology is released to a legal or natural person abroad, an export authorization will be still necessary. This amendment aims to render the use of cloud services less problematic.[47] Further interesting provisions include the applicability of controls in items contained in a person's luggage which are to be exported outside the EU, the control of technical assistance in connection with WMD or controlled military end-uses,

44 Ibid.

45 This is the result of an online survey gathering responses from forty industry practitioners. The survey ran from December 9, 2015 to January 8, 2016 and the outcomes will be made available in the doctoral study on the interferences between trade controls and research to be published in 2017.

46 Ibid.

47 However, the American approach provides for additional safeguards such as encryption of transmitted data and assurances that the cloud provider's servers are not located in restricted countries.

and the provision for an EU General Export Authorization for intra-company transfers aiming to facilitate technology and software transfers among the affiliates of a parent company.[48,49] Presumably such facilitations could also apply for transfers between research centers of the same institution if the necessary conditions are fulfilled.

The proposal does not take any steps to clarify the decontrol notes and it does not refer explicitly to the need for compliance measures by and outreach activities towards academic institutions. One could argue that the exporter definition includes also researchers and thus by extension, any consequent responsibilities concern researchers as well. From one point of view, important questions such as those raised in the H5N1 case remain unaddressed. According to an Italian officer, "as long as the EU regulation does not include an explicit reference to the role of the academic world in relation to trade controls, we lack the means to convince our hierarchy to dedicate resources so as to better tackle the problem of dual-use research."[50] However, other scholars and practitioners would rather prefer the adoption of guidelines focusing on intangible transfers and the role of academia. Interestingly, 76% of the respondents that participated in an online public consultation launched by the European Commission last summer supported the idea for some sort of guidance on this topic.[51]

The way forward towards the adoption of the new regulation is long and it requires the approval of the EU Member States and the European Parliament prior to becoming the new rule. The deliberations to come in the relevant formations of the Commission and Council are expected to be intense. As one experienced expert estimates, the final text of the regulation will maybe have little relation with the proposed one.[52] The new regulation aspiring to "generate the modern capabilities the EU needs for the coming decade" should consider ways to address satisfyingly the challenges stemming from the application of controls to research activities.[53]

The American View

US authorities have a clear and pragmatic approach to clarify the role of trade controls with regards to research. In the first place, they distinguish between inputs to research that can be controlled if covered by the Export Administration Regulation and outputs that are not

---

48 EU Commission, "Proposal for a Regulation of the European Parliament and of the Council Setting Up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (recast)," COM(2016) 616 final, Brussels, 2016, <http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154976.pdf>, see article III.

49 The formerly separate legal basis for technology—covered by the regulation—and technical assistance provided through the cross-border movement of persons—covered by the Council Joint Action 2000/401/CFSP—has been merged into the recast regulation.

50 Presentation in the 7th Export Control Working Group meeting "Complying with Trade Controls in a Research Setting," November, 2015.

51 EU Commission, "Impact Assessment: Report on the EU Export Control Policy Review Brussels," SWD (2016) 315 final, Brussels, 2016, pp. 52-53.

52 This was the experience with the former proposal amending the old dual-use regulation 1334/2001. Discussion with Pr. Dr. Quentin Michel.

53 EU Commission, "Impact Assessment: Report on the EU Export Control Policy Review Brussels," SWD (2016) 315 final, Brussels, 2016, p. 5.

controlled if no information is withheld in application of proprietary or security restrictions.[54] The distinction implies two possibilities for trade controls to come into play. The first concerns the case where existing controlled items, technical information, or software is used as input in research. This means that researchers dealing with such controlled commodities will need to comply with export and deemed export obligations applying each time. Deemed export rules in particular may require export authorizations to be in place for foreign nationals working in an American laboratory and accessing controlled information. The second possibility concerns the case where outcomes generated by research are subject to proprietary or security restrictions. Again in this case, an export authorization shall apply for releasing abroad controlled information. On the contrary, research that is to be shared broadly within the research community and for which researchers have not accepted restrictions for proprietary or national security reasons is considered as 'fundamental research' and is free from constraint.[55] The applicability of the US trade controls is described vividly in the figure I below.

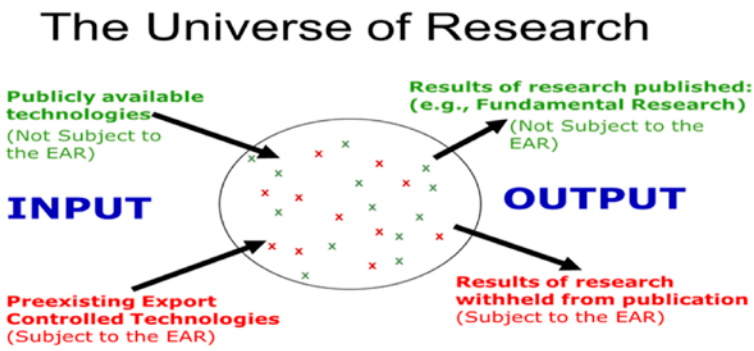

Figure I: Dealing with the dual-use research in the US context.[56]

Second, the law, as amended recently, provides that information or software arising during or resulting from fundamental research—this is the term used for basic research in the US—is excluded from the scope controls.[57] In addition, research that is consistent with prepublication reviews and obligations set under national security controls is also considered as "fundamental research" and therefore, it can be exported freely.[58] Such an approach presupposes the existence of a reliable and strong security control system by government agencies for federally funded research.

---

54 15 CFR 730-774. The Export Administration Regulations (EAR) setting the rules for the transfer and export of commercial dual-use equipment, materials and technologies, administered by the Bureau of Industry and Security (BIS) at the Department of Commerce, can be consulted in: <https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear>.

55 15 CFR §734.8 (c) as amended in December 31, 2016.

56 Figure from the presentation "The Nexus between Strategic Trade Controls and Academic Research," offered by Alexander Lopes, US DOC, in the 7th ESARDA Export Control Working Group, December 3-4, 2015.

57 15 CFR §734.8 (a).

58 See notes 1-3 in §734.8.

Third, in the same fashion that the "publishability" of research is the main criterion for applying the fundamental research exemption, the EAR defines when information and software are considered as "published" or, the "public domain exemption"[59]:

- Library collections open to the public;
- Printed books and pamphlets;
- Public posts on internet websites;
- Information distributed unlimitedly in a conference or released by instruction in a catalogue course; and
- Published patents and open patent applications.

The practical implementation of such rules does not always come at ease for universities and firms. For example, the most renowned US universities invest considerable resources and efforts in ensuring compliance with EAR and ITAR rules.[60]

On the flip side, the US approach does not consider a different contingency: what about the case where one publishes controlled or sensitive information solely with the intent to circumvent controls? Logically, most of the time a company does not have an interest in publishing commercially valuable information but the current practice may allow loopholes. In addition, whereas the fundamental research exemption intends to protect the free dissemination of information, one could ask what shall apply for fundamental research that is deemed as particularly sensitive. A plausible answer could be that trade controls cannot address all threats and indeed are not the sole instrument in place for tackling dual-use research.

The Governance of Dual-use Research

At this point it is useful to consider what mechanisms are in place or could be used for the oversight of sensitive research activities. All instruments discussed below can be considered as mutually reinforcing to trade controls yet some of them are of more direct relevance to export control objectives. The examples set forth do not represent an exhaustive compilation of existing measures or possible mechanisms for future consideration.

Measures Complementary to Trade Controls

Visa screening procedures and student vetting schemes are useful instruments aimed at ensuring that criminals or individuals of certain nationalities are not able to access particularly sensitive information. Preventing specialized teaching or training of certain nationals in disciplines relating to nuclear activities has been pursued internationally at the highest level through the

59 15 CFR §734.7.

60 This was one of the main finding in C. Charatsis, *Interferences between Nonproliferation and Science*, (forthcoming).

adoption of the United Nations Security Council resolutions 1874 (2009) and 1737 (2006) in relation to sanctions against North Korea and Iran.[61]

Although highly discriminatory, visa screening may represent a plausible approach for certain cases. As Rebolledo observes, "the structure of technical-scientific knowledge in a given state could be described as a system with inflows (imports of ITT and immigration of foreign students, technical experts, and researchers seeking scientific knowledge) and outflows (exports of ITT and emigration of national technical experts and scientific researchers seeking scientific knowledge abroad) where changes in one function would probably affect the other one."[62] In other words, what would be the added value of implementing trade controls preventing EU nationals from sharing knowledge with foreign nationals abroad when they are allowed to come to the EU and acquire sensitive knowledge?

In the US, visa screening procedures have also been considered as an alternative to the problematic application of the deemed export control rule. The deemed export notion considers that any release of controlled 'technology'—as understood in the regulations—to a foreigner within the US amounts to an export to this foreigner's country for destinations requiring an export license. The deemed export rule has been challenged as burdensome while at the same time its current interpretation allows for loopholes.[63] On the other hand, leaving the monitoring of the flow of students solely up to the visa processing system has been also considered insufficient or cumbersome.[64]

In the EU, the "New Lines for Action in Combating the Proliferation of WMD and their Delivery Systems" acknowledges the risks relating to the exploitation of knowledge and technology for malicious purposes and recommends increasing cooperation in terms of consular vigilance in order to tackle this problem.[65] In fact, EU Member States address such concerns mainly through visa screening procedures and other student vetting systems. However, one should not forget that visa policies and procedures falling primarily within the national discretion and common standards at the EU level have not been achieved so far. For short stays—up to three months—common visa procedures for the Schengen Area apply.[66] However, for longer stays, applicants are required to follow the procedures set at the national level (normally a resident

---

61 See §28 of the UN Security Council resolution 1874, S/RES/1874, New York, 2009 and §17 of the UN Security Council resolution 1737, S/RES/1737, 2006.

62 Vicente Garrido Rebolledo, "Intangible Transfers of Technology and Visa Screening in the European Union," *EU Nonproliferation Papers No. 13*, *EU Nonproliferation Consortium* (2012), p. 6, <http://www.sipri.org/research/disarmament/eu-consortium/publications/EUNPC_no%2013.pdf>.

63 For the current interpretation and effectiveness of the deemed export rule see: US Deemed Export Advisory Committee (DEAC), "The Deemed Export Rule in the Era of Globalization," Report for the Secretary of Commerce, 2007, p. 83, <https://www.fas.org/sgp/library/deemedexports.pdf>.

64 See the considerations in adopting of these alternatives: Ibid, 30-31.

65 "Council Conclusions and New Lines for Action by the European Union in Combating the Proliferation of Weapons of Mass Destruction and their Delivery Systems," Council of the European Union, December 17, 2008, <http://trade.ec.europa.eu/doclib/docs/2008/december/tradoc_141740.pdf>.

66 For more information on the Schengen Area visa policies see the website of European Commission Directorate General Home at <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen/index_en.htm>.

permit will also be required in addition to a valid visa). In practical terms, the extent to which nonproliferation screening takes place may vary from country to country.[67]

In the UK context, the Academic Technology Approval Scheme (ATAS) operated by the Foreign and Commonwealth Office exemplifies how nonproliferation can be addressed by such a means. The ATAS is a student vetting scheme for nationals who originate from countries other than the UK, EEA, or Switzerland and wish to study in a British university.[68] In practice, the ATAS certificate seeks to ensure that individuals who apply to study certain sensitive subjects do not have links to WMD programs. ATAS certificates are required in addition to the normal visa procedures only for certain post-graduate courses.

Systems in Mutual Reinforcement with Trade Controls

Whilst trade controls have traditionally focused on tackling threats originating outside the borders of a given country, there are a host of security measures for addressing in principle risks within the borders of a state. Physical protection measures for research facilities, classification policies for research having security implications or entangling proprietary rights, and best practices for IT security (encrypted emails and reliable file sharing platforms) are broader security measures having some usefulness also from an export control angle. Such measures are implemented pursuant to national statutory regulations as well as international agreements and standards set sometimes by the nonproliferation treaties' implementing organizations.[69] The IAEA is particularly active in setting such standards with universal acceptance. Concerning the proliferation of bio-chemical technologies and especially biosafety and biosecurity measures, the picture is more fragmented. In fact, there are several organizations having published guidance at both the national and international level.[70] The role of the World Health Organization is also of particular importance for life science research of dual-use concern.

Early Warning Mechanisms

Admittedly, governments can exercise control over R&D activities through schemes for funding academic research, public-private partnerships, and other industry originated projects. This is an advisable approach mainly because precautions taken at an early stage of a research

---

67 Information drawn from discussions with European Union Member State representatives in the margins of the 55th Dual-Use Coordination Group meeting, September 24, 2015.

68 For more information on ATAS see the webpage of the United Kingdom government: <https://www.gov.uk/guidance/academic-technology-approval-scheme>.

69 For instance, the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" of 2001 United States Patriot Act and guidance such as the "NIH Guidelines on Research Involving Recombinant or Synthetic Nucleic Acid Molecules," National Institutes for Health, 2016, <http://osp.od.nih.gov/sites/default/files/resources/NIH_Guidelines.pdf> are notable examples of security and safety rules applying to federally funded bio-technology research in the US. For an overview of the US biosafety and security governance measures for sensitive life science research see Jonathan B. Tucker, *Innovation, Dual-use, and Security, Managing the Risks of Emerging Biological and Chemical Technologies* (Cambridge: The MIT Press, 2012), pp. 49-55.

70 Indicatively see: Peter Clevestig, *Handbook of Applied Bio-Security for Life Science Laboratories* (Stockholm SIPRI, 2009); The Dutch Royal Netherlands Academy of Arts and Sciences (KNAW), *The Code of Conduct for Biosecurity* (Amsterdam: KNAW, 2008).

project can benefit its smooth and secure execution all along its life cycle. Most governments apply specific national controls and classification schemes for defense or military-oriented research, for example. It should be noted that classification policies are presented quite often as an alternative to trade control measures. Researchers, coming especially from countries known to apply strict classification systems, have noticed that such an approach could eventually lead to over classification and more rigid restrictions compared to trade control requirements.[71] Therefore, it is advisable to use such measures only when necessary and in a moderate way.

In the EU context, the evaluation system for proposals submitted for funding in the framework of Horizon 2020 comprises an "ethics appraisal screening" including assessments for dual-use research in the meaning of the regulation.[72] It is notable that the H2020 national experts in charge of assessing such proposals use the Technology Readiness Level (TRL) metric in order to estimate the imminence of a research project to deliver a practical application of dual-use concern.[73]

Furthermore, in the life sciences, the oversight of dual-use research may rely on government committees and advisory bodies composed by both academic and security experts who are called upon to assess risks and benefits of sensitive research at any stage of a project. One could mention the American NSABB and the Dutch Biosecurity Office set up in 2009 and 2013 respectively.[74] It is notable that the competencies and status of such boards may differ. For example, while the Dutch Biosecurity Office is responsible mainly for awareness raising activities and policy support, the Danish Centre for Biosecurity and Bio-Preparedness (CBB) is also in charge of licensing for bio-related research.[75]

Contrary to early warning mechanisms, the editorial boards of journals or the reviewers involved in the peer review process could report to responsible authorities or university committees their concerns in the event of an alarming publication requiring possibly a cost-benefit analysis.

Self-governance Measures

Governmental oversight works in synergy with internal measures adopted by research institutions and industry. These efforts are either voluntary or at times represent statutory obligations. In this category belong codes of conduct, ethics committees, and internal regulations adopted by universities. In Belgium for example, the University of Leuven (KUL) has set up separate committees in charge of different aspects of research such as medical ethics, social and societal ethics, laboratory experimentation, data privacy, scientific integrity, and most interestingly,

---

71 Discussions with bio-experts in the context of 3rd Annual Conference on the "Impact of Export Controls on Higher Education & Scientific Institutions" organized by AUECO and the University of Virginia.

72 The Ethics Appraisal procedure differentiates presently between dual-use research as understood in the regulation, research with exclusive focus on civil applications and research results that can be misapplied. Security concerns were addressed also in the FP7 in the context of ethics review; however at the time there was no such differentiation.

73 The TRLs metric was first developed by NASA scientists in 1970s and the updated version is available in: <https://www.nasa.gov/directorates/heo/scan/engineering/technology/txt_accordion1.html>.

74 For more information visit the websites of NSABB and Dutch Biosecurity Office in: <http://osp.od.nih.gov/office-biotechnology-activities/biosecurity/nsabb>; <http://www.bureaubiosecurity.nl/en>.

75 Information retrieved from the website of CBB in: <https://www.biosikring.dk/home/>.

dual-use research.[76] Especially for life science research involving clinical trials and animals testing, guidance documents and codes of conduct are provided by international organizations and university networks while many universities have approval committees in place.[77] In relation to this, funding organizations such as the Economic and Social Research Council (ESRC) in the UK may require universities to have some kind of internal mechanism for ethical review of all research funded under their frameworks. Other internal measures take the form of so-called "Technology Control Plans" (TCPs) monitoring who has access to what information and ensuring that sensitive information is not exported to unauthorized users either on-site or abroad. Although generally such measures are taken voluntarily by research organizations and firms, the application of strict related legislation can indirectly trigger the implementation of internal compliance mechanisms.

Moreover, the role of National Academies and Research Councils is highly relevant to the governance of dual-use research. Presently, their contribution includes ad hoc policy support advice and guidelines for implementing self-regulatory measures. For instance, the Dutch Royal Academy of Arts and Sciences published a report as early as 2013 for improving biosecurity and the European Academies Science Advisory Council (EASAC) prepared a special report dedicated to concerns about "gain of function research."[78] Logically, the adoption of guidance and standards by academic associations must be well received by the academic community.

Conclusion: Contemplating the Role of Trade Controls for the Governance of Dual-use Research

The present paper considers a number of issues pertaining to the governance of dual-use research. More than an account of all issues addressed, this concluding section attempts to respond to whether trade controls are a "fit for purpose" instrument as regards the oversight of dual-use research and what initiatives could be taken for increasing the clout and leverage of trade controls towards dual-use research.

Building a WMD requires at least three elements: (1) special material (2) technological equipment and related knowledge (3) explicit information and technical expertise.[79] It can be argued that among the three, the element posing the greatest difficulty to acquisition is tacit knowledge but this varies depending on a weapon's type and performance capabilities of a

---

76 The relevant information can be found in the KUL website <https://www.kuleuven.be/english/research/integrity/committees>.

77 Indicatively see "Responsible Life Sciences Research for Global Health Security: A Guidance Document," World Health Organization, Geneva, 2010, <http://apps.who.int/iris/bitstream/10665/70507/1/WHO_HSE_GAR_BDP_2010.2_eng.pdf>.

78 "Improving Biosecurity, Assessment of Dual-use Research," Royal Netherlands Academy of Arts and Sciences, 2013, <https://www.knaw.nl/shared/resources/actueel/publicaties/pdf/advies-biosecurity-engels-web>; "Gain of Function: Experimental Applications Relating to Potentially Pandemic Pathogens," German National Academy of Sciences Leopoldina for EASAC, 2015, <http://www.easac.eu/home/reports-and-statements/detail-view/article/easac-report-1.html>.

79 The impact of an attack involving a WMD will also depend, apart from the destructive power of the weapon itself, on the capacity of the means of delivery.

weapon.[80] Consequently, it is legitimate to include technology (technical data and assistance) and software in the scope of trade controls.

As explained above, trade controls were not designed to oversee the conduct of all different types of dual-use research. They just represent a means to control certain research activities falling within the scope of controls and thus the term "export controlled research" may be more pertinent in this context. Without overstating the relevance of trade controls for dual-use governance, the benefits for the latter are multiple. Trade controls function as a safeguard for certain types of activities that can be misused and offer many opportunities for reinforcing the accountability of research organizations originating in either the academic or industrial context. Importantly, the practical implementation of trade controls could act synergistically with physical protection, safety, and other security measures founding thereby a net for the prevention of different types of threats.

Bearing this in mind, activities undertaken in the framework of the United Nations Security Council resolution 1540 Committee could increase the research community's awareness and generate added value for other security objectives, too. In addition, enhanced cooperation coordinated at the level of MECRs could improve the present implementation of technology controls among participating states. For example, a possible agreement of participating states upon common guidelines or standards for technology transfers in a research context could have high resonance among the key stakeholders concerned. In relation to this, reaching out to non-participating countries and communicating best practices could benefit the international harmonization of controls.

Trade controls do not intend to hinder unduly the free dissemination and diffusion of peaceful research. This needs to be made clear to the greatest extent possible by clarifying the decontrol notes and their application, preferably at international level. The EU Member States do not have unlimited possibilities to consider in this regard. They could opt for one of the following:

- Follow the US paradigm by exempting from the scope of controls all publishable research that respects security and proprietary classifications;
- Continue applying trade controls as an ad hoc manner for the assessment of research of dual-use concern as Dutch have done in the H5N1 case; or
- Establish a *sui generis* methodology for evaluating sensitive research based on criteria such as the overall utility, sensitivity and the readiness of research to be misapplied.

It must be acknowledged that the proliferation of WMD has occurred in the past and its continuing practice could harm the overall credibility of trade controls as a nonproliferation tool. Trade controls, as any other security measure, cannot respond to every threat. The realistic contemplation of the world suggests that different asymmetric factors need to be considered. For example, an irrational or determinant actor can always find a way to circumvent a security measure. However, these acknowledgments should not be used as an excuse for underestimating the contribution of trade controls in meeting security objectives.

---

80 Jonathan B. Tucker, *Innovation, Dual-use, and Security, Managing the Risks of Emerging Biological and Chemical Technologies* (Cambridge: The MIT Press, 2012), p. 23.

Above all, the dual-use problem of technology relates to an underestimated aspect: the education and training of the next generation of scientists on the security implications potentially connected to the development of emerging technologies. Such training could include export control concepts and principles and should also aim at developing the ethos and character of researchers in confronting dual-use dilemmas.

Export Control Compliance and American Academia

BRIAN STARKS AND CHRISTOPHER TUCKER[1]

Abstract

Export control compliance typically centers on the efforts by industry to comply with export control regulations worldwide. However, academic institutions are increasingly finding themselves under government scrutiny for possible export control liability. This paper describes the challenges faced by American academic institutions in complying with United States export controls and highlights case studies of major export control violations by US academic institutions as well as their efforts to adopt, shape, and modify industry compliance models to an academic culture. This analysis emphasizes how the changing landscape of research funding can increase export control compliance implications for American universities. The paper concludes with a discussion of new institutions that are developing to assist academia in meeting export control challenges.

Keywords:

Academia, export control compliance, universities, export control, security culture

1 Brian Starks is a Research Assistant at the Center for International Trade and Security (CITS) and a Ph.D. student at the University of Georgia's School for Public and International Affairs (SPIA). Prior to becoming a CITS Research Assistant, he worked as an export compliance specialist at an aerospace company, focusing on government authorization applications. Brian's current research focuses on strategic trade control legislation, implementation, and enforcement. Christopher Tucker is a Research Associate at the Center for International Trade and Security (CITS). Christopher is a trainer and project coordinator for the twice annual Security and Strategic Trade Management Academy (SSTMA). Christopher regularly provides training on strategic trade control issues related to licensing and government-industry cooperation. Christopher's current research focuses on strategic trade control implementation and UNSCR 1540 compliance.

Introduction - Security Culture comes to American Academia

Modern export control regulations have affected strategic industries since the early days of the Cold War. For much of this time, governments largely concerned themselves with regulating international trade in arms and dual-use goods. As globalization and technological advancements grew at an ever-increasing pace, export controls became a concern for all companies. Whether a company manufactures missiles, nickel powder, or telecommunications software, they must remain cognizant of export control regulatory requirements. While industry's export compliance obligations are well-known, another key source of strategic items has historically received noticeably less regulatory attention: higher education at various universities and colleges. Note that while many countries' strategic trade regulations affect domestic education institutions, this article will focus solely on the American export control system and its impact on universities located in the United States. Existing publications well describe European universities' export compliance challenges, but lack specific case studies detailing violations.[2]

Universities and arms manufacturers alike must comply with the same complex export regulations. Unfortunately, much of contemporary export compliance materials focus on corporations' challenges exclusively. Literature for university export compliance is relatively sparse when compared to private sector resources.[3,4] Some universities have run afoul of these regulations, resulting in high profile violations. Specifically, since existing regulations and available resources focus on private sector compliance, higher education and research institutions can struggle to properly apply nuances pertaining to deemed exports, intangible technology transfers, and denied party screening.[5,6] These violations come with both financial and reputational penalties, harming institutions' long-term interests.

Despite the shared regulatory burdens between industry and academia, significant differences result in disparate implementation strategies. Each institution's unique traits require a bespoke export control program, tailored to maintain regulatory compliance while balancing the myriad of other university responsibilities. The institution's research interests and degree of centralization drive how the university structures its export compliance department. Additionally, certain research areas, such as encryption or biological pathogens, may entail further restrictions on participants' nationalities and whether the findings can be published for wide distribution in an academic journal.

---

2 "Workshop: Dual-use Export Controls," Policy Department, Directorate-General for External Policies, European Parliament, October 2015, <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/535000/EXPO_STU(2015)535000_EN.pdf>.

3 For a thorough discussion of university export compliance, refer to Brady, Peloso & Rowold, "Export compliance and secure research," in A. Dade, L. Olafson, S. M. DiBella, eds, *Implementing a Comprehensive Research Compliance Program: A Handbook for Research Officers* (New York: Springer, 2015), pp. 249-303.

4 Various law journals have addressed university export compliance, although some sources are partially outdated after 2013's Export Control Reform efforts. Refer to Rege, R. "Universities Should Implement Internal Control Programs to Monitor Compliance with Export Control Laws," *Journal Of Law & Education* 35 (April 2006), p. 199.

5 "Deemed Exports," as defined under 15 CFR §734.13(a)(2) of the Export Administration Regulations (EAR), refer to the transfer of technology (or source code) to a foreign person located in the United States.

6 "Intangible Technology Transfers" include but are not limited to email, electronic documents, presentations, visual disclosure, and even technical discussions over the phone or in-person.

Recent trends in higher education portend an increasingly significant role for university export compliance programs. The most prominent shifts include: changes in research funding, student demographics, and larger institutions' increasingly globalized portfolio. Much like how export control regulations began as something afflicting cottage industries and, as value chains became segmented, spread to larger multinational corporations, academic institutions are now experiencing new pressures that necessitate the adoption of wide sweeping export compliance policies.

Lastly, renewed interest in university export compliance requires a common forum. For years, government outreach efforts focused on private sector audiences rather than academia, partially due to the difficulty in finding an appropriate forum or organization to help coordinate on behalf of university compliance professionals. Specific professional organizations and conferences have emerged in recent years to promote the sharing of best practices, provide benchmarking, and promote a professional community among university compliance officers. Government agencies have taken notice, finding it more efficient to engage directly with university compliance officers via these niche professional avenues.

Clashing Cultures - Export Restrictions vs. Journal Publications

Government regulatory requirements and academic research culture are, at times, diametrically opposed. The regulations apply to nearly every facet of a scholar's career, from publishing research, attending conferences, incorporating foreign research partners, and designing seemingly routine international research collaborations. Professors operate in a "publish or perish" environment, encouraging them to pursue new, innovative research and publish findings for widespread dissemination. The bigger the breakthrough and publication's audience, the better for the scholar's career. However, from initial brainstorming to future publications, regulatory requirements create potential pitfalls. Three case studies exemplify different nuances that can go unnoticed yet lead to significant violations for unwary universities.

Professor Roth, University of Tennessee - Deemed Export & Travel Restrictions

In September 2008, Dr. John Roth, a former University of Tennessee professor, was the first professor charged with violating United States export regulations. The United States Air Force (USAF) contracted Dr. Roth to develop specialized plasma technology for use on unmanned aerial vehicles (UAVs).[7] This project, highly technical and specifically for military purposes, fell under strict export restrictions which would have required explicit State Department approval prior to any foreign national participation. Despite prior knowledge of these regulations, Dr. Roth enlisted Chinese and Iranian graduate students to work on the USAF contract, resulting in deemed export violations. Furthermore, Dr. Roth brought a laptop containing sensitive military technology to China while attending a conference. Former colleagues told investigators that Dr. Roth disregarded export controls' utility and found them overly restrictive, which contributed to his decision to flout the regulations.

---

7 "Retired University Professor Sentenced to Four Years in Prison for Arms Export Violations Involving Citizen of China," Office of Public Affairs, United States Department of Justice, July 2009, <https://www.justice.gov/opa/pr/retired-university-professor-sentenced-four-years-prison-arms-export-violations-involving>.

Upon returning to America, government authorities stopped him at the Detroit airport to make copies of the documents Dr. Roth brought to China. After confirming that the documents contained restricted information, the Federal Bureau of Investigation (FBI) received a warrant to seize Dr. Roth's laptop and thumb drive. Despite no evidence suggesting that Dr. Roth transferred the technology to any party while abroad, merely traveling to China with the USAF technology is a direct violation of United States export regulations. In 2009, Dr. Roth was found guilty of conspiracy, wire fraud, and 15 counts of exporting "defense articles and services" to foreign nationals. Dr. Roth was the first professor to receive incarceration time for export violations; this would soon prove to be a wake-up call for many universities across America to critically evaluate their own export compliance policies.

Lapse in Military Technology Control Leads to Illegal Access

At the Georgia Institute of Technology (Georgia Tech), a widely recognized and prestigious engineering school, there was an inadvertent yet serious mishandling of military technology.[8] A professor who conducted a class involving infrared technology used in weapons-aiming systems for aircraft, ships, and tanks was retiring. His course, given the involvement of restricted military data, was open to US citizens only. The professor asked university staff to copy his course materials to a DVD so that it could be given to a colleague who could teach that course after he retired. After experiencing technical difficulties transferring the information to a DVD, the Georgia Tech media staff made the course available via an internet link. Unbeknownst to the media staff, the link was open to the public.

Despite the robust export compliance program in place at the time, the release of controlled technology occurred. Although a temporary lapse in compliance policy and an honest mistake, for over two weeks internet users in 36 different countries (including China, Russia, Iran, and Pakistan) downloaded the restricted data. Georgia Tech voluntarily self-disclosed the event to the United States Department of State, which responded with a strongly worded reprimand.

Ultimately no penalties were assessed due to Georgia Tech's voluntary disclosure, full cooperation with State Department authorities, and immediate improvements made to their university compliance program. To date, this program serves as an ideal model for universities conducting highly advanced and restricted research. A recent Georgia Tech publication thoroughly discusses the current export compliance program, covering its structure, implementation, and unique challenges resulting from its position as a global leader in technical research.[9]

The case serves as a cautionary tale that all university staff must remain cognizant of export controls, especially when pertaining to intangible technology controls. In the unfortunate event in which universities violate these regulations, they should emulate Georgia Tech's response, voluntarily disclosing and fully cooperating with government regulators.

---

8 Daniel Golden, "Military Secrets Leak From US Universities With Rules Flouted," Bloomberg News, April 30, 2012, <https://www.bloomberg.com/news/articles/2012-04-30/military-secrets-leak-from-u-s-universities-with-rules-flouted>.

9 John Krige, "Regulating the Academic "Marketplace of Ideas": Commercialization, Export Controls, and Counterintelligence," *Engaging Science, Technology, and Society* 1, (2015), pp. 1-24.

International Collaboration Leads to Screening Failure

The University of Massachusetts at Lowell (UML) suffered the unfortunate consequences of insufficient party screening prior to international collaboration. In 2009, employees from UML and Pakistan's Space and Upper Atmosphere Research Commission (SUPARCO) co-authored a technical paper analyzing electron density in Karachi and Islamabad.[10] Presumably during the research, UML exported atmospheric testing equipment to SUPARCO.

The equipment is not typically controlled by export regulations, but UML failed to realize that the United States government had placed SUPARCO on the Department of Commerce's Entity List, which establishes additional export requirements for entities suspected to engage in proliferation activities.[11] The United States government must approve an export application prior to nearly all shipments to an entity listed under the Department of Commerce's list. Ultimately, the United States government assessed UML a $100,000 USD civil penalty which would be waived after two years without additional export violations.[12]

Differences between Academia and Industry

Traditionally, strategic traders try to act proactively in conducting export compliance, meaning large corporations implement measures to screen customers, screen geographic areas of concern, conduct training, and enact standard operating procedures to prevent bureaucratic mistakes that lead to violations. The hierarchical structure of most corporations allows for a high degree of centralization for export compliance functions. Prior to new transactions, the export compliance department will often need to sign off to ensure that all the relevant regulatory obligations have been observed.

In academia, however, the response to export compliance has been largely reactive. In the wake of a violation or the wake of a violation by nearby or partner institutions, a university will often begin assessing compliance capacity, identifying existing risks, and developing preventative measures. This assessment guides the university as it establishes an export compliance office, with customized procedures and functions to best accommodate the institution's characteristics. In stark contrast to corporate compliance functions, the university counterpart faces a much more open, decentralized mode of operation. Academic institutions' culture and organization tend to contain fewer bureaucratic checks and standard operating procedures.

If the university compliance office does not have proper training curricula and outreach for faculty, researchers may be inadvertently violating export regulations. As the Roth case demonstrated, foreign national students working on-site can still pose considerable risk. By honest mistake, the Georgia Tech media staff placed controlled information in a publicly

---

10 G. Murtaza, S. Iqbal, M. Ameen, & A. Iqbal, "Comparing IRI and a Regional Model with Ionosonde Measurements in Pakistan," *Advances In Space Research* 42:4 (August 18, 2008), pp. 682-690, <http://adsabs.harvard.edu/abs/2009AdSpR..43.1821A>.

11 The Entity List can be found at: <https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list>.

12 Bureau of Industry and Security & UML Settlement Agreement, May 2013, <https://www.oesrc.researchcompliance.vt.edu/sites/oesrc.researchcompliance.vt.edu/files/umasslowell_e2306.pdf>.

available location. UML may have determined the research equipment was not under export control under normal circumstances, but failed to realize the end-user was on the Entity List. While export compliance departments can never eliminate all risk, properly tailored training and outreach allow university employees and students to understand their obligations and how to proceed accordingly.

To demonstrate the importance of routine training, awareness, and compliance process requirements, an American university compliance officer spoke of the sanctions hurdles when attending academic conferences in Iran. The Iranian Transactions and Sanctions Regulations require a license from the Treasury Department for a wide variety of activities, including participation in academic conferences in Iran.[13] With less than ideal notice, faculty submitted their international travel request, which was reviewed by the compliance officer. The faculty were not in departments with traditional export control risk and, when initially planning the trip, had not reviewed the institution's export compliance or international travel webpages nor discussed the travel with any of the units associated with approving international travel. Additionally, unbeknownst to the faculty, the Treasury Department rarely approves license applications quickly. The faculty had mistakenly assumed that there were no problems with engaging in academic activities, such as conferences, in Iran, until they became aware of the complexities behind sanctions regulations and Department of Treasury licensing. The university compliance officer was able to apply for and receive a Specific License for the institution's faculty members to proceed with their planned activities on schedule.

Reported university export violations are few and far between, preventing an accurate and in-depth appraisal of academia's overall compliance.[14,15] However, those known cases are egregious enough to warrant attention from the rest of the academic community, prospective outside funders, and government regulators. An export compliance officer, much less a staffed office, has always been a necessity at any large research institution, but it's also becoming increasingly relevant for smaller schools with technical programs or overseas affiliations. Academic institutions are now engaging in more international collaborations that go beyond the traditional study abroad programs; universities continue to build satellite campuses overseas, laboratories, and partnerships with foreign corporations. As the University of Massachusetts at Lowell discovered, proper screening mechanisms and due diligence can identify potentially risky international collaborations.

Prior to these infamous violations, export compliance duties were vested in a legal office or another regulatory compliance office. A professor seeking to undertake an international collaboration may have needed to consult with the university legal office before transmitting

---

13 "Iranian Transactions Regulations (31 C.F.R. PART 560) Statement Of Licensing Policy On Support Of Democracy And Human Rights In Iran And Academic And Cultural Exchange Programs," United States Office of Foreign Asset Control, July 6, 2006, <https://www.treasury.gov/resource-center/sanctions/Programs/Documents/license_pol.pdf>.

14 Supporting the claim of under-reported university compliance mistakes, the Commerce Department's Bureau of Industry and Security releases periodic collections of export violations. The September 2016 Edition contains over 90 case studies, with only two examples originating from American universities. The remaining case studies concern either individual actors or private corporation.

15 "Don't Let This Happen to You!," United States Bureau of Industry and Security, September 2016, <https://www.bis.doc.gov/index.php/forms-documents/enforcement/1005-don-t-let-this-happen-to-you-1/file>.

data or information that could be considered intellectual property to the university. The onus would be on the legal office to screen the transfer or collaboration for any export control issues as part of evaluating the profit motive behind the transfer or collaboration. For example, if a scientist wanted to transfer data to an overseas partner, they may have needed to ask the university for permission under the guise of preserving intellectual property, but the university legal offices may have discovered the international partner is on a sanctions list or has possible ties to denied parties.

As corporations have experienced, the United States government and increasingly foreign governments are putting the onus of responsibility for export compliance on the exporter.[16,17] US government officials often refer to industry as the "first line of defense" in secure trade, often dismissing ignorance of the law as a mitigating factor. Regulators feel that advanced technology comes with stewardship responsibilities which companies underemphasize at their own peril. That "first line of defense" onus extends beyond the corporate world and into the academic community as well, promoting a proactive export compliance culture for universities.

Academic institutions, much like the private sector, are concerned with more than the direct financial penalties of a violation. The reputational damage and the message conveyed to possible outside funders, much like vendors/customers in the corporate world, acts as the true deterrent for academia. This rings particularly true for institutions who commonly receive highly technical contracts from various military organizations. Georgia Tech immediately self-disclosed their violation, as well as implementing measures to prevent another such mistake from occurring again. Georgia Tech's robust export compliance demonstrates to the USAF that it will remain a trustworthy steward of advanced military contracts.

To FRE or not to FRE

The Fundamental Research Exclusion (FRE) permits universities a degree of freedom from export control's burdens.[18] The FRE allows US academic institutions' foreign faculty and students to participate in research involving would-be restricted information, while on campus, without receiving a deemed export license from the United States government. There are several important requirements that fall under the FRE, making the exclusion either a powerful tool if implemented properly or a risky assumption if poorly understood. Per the Bureau of Industry and Security (BIS), the results must be "published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or

16 As a private sector example of improper intangible technology controls, Intevac, a California company specializing in thin film deposition and sensor technologies, failed to properly safeguard technology controlled for National Security, Nuclear Proliferation, and Missile Technology reasons. Intevac disclosed restricted information to a Russian employee, resulting in an illegal deemed export. Furthermore, Intevac lacked proper information technology policies to prevent its Chinese subsidiary from accessing the controlled technology. While there was no malicious intent behind Intevac's actions, the United States government assessed Intevac $115,00 USD in civil penalties.

17 United States Bureau of Industry and Security & Intevac Settlement Agreement, February 2014, <https://efoia.bis.doc.gov/index.php/documents/export-violations/export-violations-2014/922-e2365/file>.

18 FRE is defined in 15 CFR §734.8(a) and 22 CFR §120.11(a)(8), under the EAR and International Traffic in Arms Regulations (ITAR), respectively.

national security reasons."[19] Furthermore, the exclusion does not authorize the transfer of export controlled commodities abroad, even to foreign research partners. Given the FRE's complexities, many institutions' export compliance offices have dedicated resources to provide faculty and staff with detailed explanations for how the FRE is used in their organization.[20]

Some institutions' export compliance officers speak of a *de facto* policy to pursue FRE-eligible research almost exclusively. While FRE eligibility does not remove all export control risk, such as restricted parties screening requirements, it can alleviate many faculty concerns regarding publication or international conference presentations. Furthermore, FRE-only research reduces the overall compliance burden for the export control departments, allowing them to successfully operate with fewer devoted resources when compared to their counterparts with more restricted research programs. Often these "FRE Only" policies originate from the specific institutions' research profile, favoring basic research compared to advanced, applied research. Given the specific nature of applied research, restrictions on publication are more likely when private sector or military partners fund the projects. As the academic disciplines and funding environment continues to change over time, institutions may find themselves at a crossroads- remain *de facto* FRE-only, with less funding opportunities, or take on new, non-FRE research projects and their accompanying export controls? Universities who decide to pursue more restricted research must take care to review their export compliance programs due to the significant increase in stringent regulatory obligations once FRE no longer applies.

Trends in Academia, Increasing Role for Export Compliance

Truly, academia itself is evolving to meet modern challenges in research and learning. This evolution causes a greater need to be cognizant of export regulations due to frequent technology transfers. As more researchers travel to sanctioned countries and areas of concern, there are challenges with technology control, jurisdictional responsibility, and possible cyber threats. Not just concerning travel, but an increasing amount of actual teaching and transfer of course materials takes place online, many times to students or other participants overseas. Universities are now under increased pressures to produce online courses and online course materials for sale to a larger student marketplace. Tele-learning is becoming as popular as tele-working and frequently, students in technical fields pursue online certificates to keep current with modern technology, which in some cases may be controlled technology.

Contrasting with the increasingly globalized academic system, traditional research funding sources face more significant resource constraints than ever before. For example, between 2003 and 2015, the National Institute of Health (NIH) lost 22% of its ability to provide funding for research across the United States.[21] Federal funds will likely only increase in scarcity in

---

19 "Deemed Exports and Fundamental Research for Biological Items," United States Bureau of Industry and Security (BIS) website, <https://www.bis.doc.gov/index.php/policy-guidance/product-guidance/chemical-and-biological-controls/14-policy-guidance/deemed-exports/111-deemed-export-and-fundamental-research-for-biological-items>.

20 For example, the Massachusetts Institute of Technology's Office of Sponsored Programs, University of California, Los Angeles, and University of Iowa all maintain guidance using the FRE.

21 "NIH Research Funding Trends," Federation of American Societies for Experimental Biology, <http://faseb.org/Science-Policy-and-Advocacy/Federal-Funding-Data/NIH-Research-Funding-Trends.aspx>.

the near term, as President Donald Trump announced a proposed budget that would reduce federal funding for a variety of research. Among the federal programs with reduced budgets, the NIH stands to lose $5.8 billion (18%) from its current funding level.[22] Increasingly common budget cuts and sequestration result in fewer NIH-sponsored projects, creating a funding gap that universities may seek to alleviate with more controlled research programs. As it stands currently, the Georgia Tech publication provides a rough estimate that "no more than perhaps 5-10% of sponsored contracts deal with sensitive but unclassified knowledge that is subject to export controls or related restrictions."[23] Given the shrinking pool of federal research resources, it is possible that this estimate will soon need to be updated as more institutions turn to more restricted opportunities.

The NIH often funds projects which will be covered under the Fundamental Research Exclusion, providing those NIH-recipients a high degree of export compliance freedom. Universities' research efforts could face increased export control-related obligations if new, more restrictive partnerships formed with other government organizations (i.e., the USAF) or private corporations. The Department of Defense (DOD) funds a variety of university projects, some which fall under the FRE while other efforts remain highly controlled. As a contrast to the University of Tennessee's restricted USAF research, a university could receive DOD funds to study wildlife impacts on a US military installation. This type of project is unlikely to contain export controlled technology and is likely to be considered fundamental research, which would allow the university researchers to freely publish and disseminate their findings without restrictions on foreign national participation.

Emergence of Professional Forums

After the Roth case's watershed moment, many academic institutions took a renewed interest in their own compliance programs.[24] New export control offices and positions grew more commonplace on professional networking websites, reflecting a growing need for export professionals at universities. The desire for professional forums quickly arose as additional universities established trade compliance offices. At the time, export compliance associations and conferences were almost entirely tailored for private sector audiences, which can be poorly suited to university compliance officers given the vast differences between corporate and academic organizations.

A few years ago, a group of university export compliance officers created the Association of University Export Compliance Officers (AUECO).[25] Per the AUECO website, the association

---

22 "America First, A Budget to Make America Great Again," United States Office of Management and Budget, March 12, 2017, <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/budget/fy2018/2018_blueprint.pdf>.

23 John Krige, "Regulating the Academic "Marketplace of Ideas": Commercialization, Export Controls, and Counterintelligence," *Engaging Science, Technology, and Society* 1, (2015), pp. 14.

24 As evidence of its widespread impact, numerous university export compliance resources specifically mention the Dr. Roth case such as the Ohio State University, Pennsylvania State University, University of Wisconsin-Madison, and the Texas A&M University System.

25 AUECO's website can be found at: <http://aueco.org/>.

seeks to develop a shared community to "associate," "advocate," and "collaborate." Initially, the organization consisted of roughly 20 members. Since its inception, AUECO has grown to over 170 members from over 110 institutions. The association benefits members by publishing guidance papers, creating a members-only forum, advocating for improved government-academia communications, and perhaps most importantly- helping promote an annual university compliance conference since 2013.

These conferences, organized by individual host universities, bring together university compliance officers and government officials. While AUECO does not host the event, it strongly encourages its members to attend. These conferences allow easier networking and sharing of best practices among university compliance professionals, which can be especially beneficial for those who serve as their institution's only export compliance specialist. Government officials use these conferences as a rare opportunity to conduct university-centric training and outreach, which was challenging prior to AUECO. The regulatory agencies (typically Commerce, State, and Treasury) simply lack the resources to coordinate and sustain outreach and training events that would provide them with such a large audience of university export compliance staff. Officials use these conferences to highlight how their regulations specifically affect universities, receive feedback, answer questions, and prove customized training that would be absent at typical industry outreach events.

Presumably recognizing the same dearth of university export events behind AUECO, private companies have developed tools, resources, and curricula tailored to the unique compliance challenges facing American universities today.[26] One such company, for example, began conducting annual University Export Control conferences in 2016, tailoring seminars for universities, laboratories, other scientific institutions, US government organizations, and private corporations working with universities or laboratories.[27]

Balancing Cutting-Edge Research & Ensuring Export Compliance

Given the unique challenges facing university export compliance programs, it is apparent that private sectors policies will not be sufficient. As the above case studies demonstrate, there are a myriad of pitfalls that could lead to costly export violations. Dr. Roth's flagrant disregard for the University of Tennessee's export compliance training illustrates the increased risk of decentralized universities, as compared to the traditionally more centralized industry actors. Despite an existing export compliance program, Georgia Tech media staff's momentary lapse led to the dissemination of military technology to prohibited countries. While Georgia Tech's voluntary disclosure and subsequent actions helped mitigate reputational damage, it remains a valuable reminder that export compliance programs can mitigate but never eliminate risk. UML learned that seemingly innocuous research can result in violations due to the potential restricted nature of international partners.

---

26 "University Export Control," Export Compliance Training Institute, <http://www.learnexportcompliance.com/Seminars/University-Export-Controls.aspx>.

27 "Recent & Past Events," Export Compliance Training Institute, <http://www.learnexportcompliance.com/Seminars/Recent-amp;-Past-Events.aspx>.

These case studies exemplify just some of the potential export compliance mistakes that bring increased liability to universities. Advanced technical research, international partnerships, restricted funding projects, large foreign national student populations, data management, and genuine "academic culture" all come with higher risk. There is no "one size fit all" approach with export compliance; each institution must carefully assess its current and future state to promote a proactive compliance culture.

Universities should remember that they are not expected to navigate these complex regulations alone. As the American government has grown increasingly interested in enforcing academia's export violations, it has also devoted more resources to the training and education of universities regarding their obligations. In addition to governmental support, universities can take advantage of recently created organizations to further refine their own export compliance programs. Given the combination of increasingly globalized academic institutions and diminishing federally-funded research opportunities, robust export compliance programs may soon become key strategic offices at universities across America.

The Proliferation of Cyber-Surveillance Technologies: Challenges and Prospects for Strengthened Export Controls

FABIAN BOHNENBERGER[1]

Abstract

The global trade in cyber-surveillance technologies has largely evaded public scrutiny and remains poorly understood and regulated. European companies play a central role in the proliferation of a broad spectrum of advanced surveillance systems that have legitimate uses, but have also been repurposed for nefarious ends. Export controls have become an important instrument to restrict sales of cyber-surveillance equipment and software to repressive regimes; however, these technologies pose significant challenges to traditional frameworks for the control of dual-use exports. This article provides an overview of current developments on the European level and within the multilateral Wassenaar Arrangement and presents the current state of export controls on cyber-surveillance technology. Most importantly, it discusses the outcome of the European Union export control policy review, focusing on the regulation proposed by the European Commission in September 2016, and provides an initial assessment of the key innovations and limitations of the draft text. In addition, the article presents an analysis of the current debate regarding the problematic definition of "intrusion software" in the Wassenaar Arrangement and offers insights into some alternative proposals.

Keywords

ICT surveillance systems, export controls, Wassenaar Arrangement, human rights, European Union, EU Dual-use Regulation, policy review

1 Fabian Bohnenberger recently completed his Master of Public Policy at the Hertie School of Governance in Berlin. For his Master's thesis on export controls for cyber-surveillance technologies he received an 'Aquila ascendens' young academics award for security policy in April 2017. His research focuses on international trade relations, the application and effects of sanctions and export controls, and the democratic legitimation of transnational governance.

Introduction

Increasing exports of advanced surveillance capabilities have become a focus of controversy and debate on regulatory and legal controls that can be used to limit sales to governments with dubious human rights records. European companies play a central role in the proliferation of a broad spectrum of systems for targeted and mass surveillance that are used to observe and analyze behaviors and identities of people on computers, mobile phones, and telecommunications networks. These technologies have legitimate uses but have also been repurposed by some authorities to contribute to serious human rights abuses, the suppression of journalism and civil society, and the persecution of human rights defenders, dissidents, and political opponents.[2]

Export controls today represent an important instrument to restrict sales of cyber-surveillance equipment and software to repressive regimes; however, these technologies pose considerable challenges to traditional frameworks for the control of dual-use exports. Actors in the debate offer different conceptions of what technologies or services should be subject to export authorization requirements, why these items (and not others) should be controlled, and what an effective control regime would look like. On September 28, 2016, the European Commission introduced a proposal to update the European Union Dual-Use Regulation, which includes new provisions on the export of cyber-surveillance technologies.[3] The Commission's draft will be discussed and decided upon by the European Council and the European Parliament in the ordinary legislative procedure. The Committee for International Trade (INTA), which is responsible for drafting the Parliament's position, held an initial public hearing on the dual-use reform on March 21, 2017, but it is not yet known when the regulation, if adopted, is expected to enter into force.[4,5] Concurrently, however, existing provisions on cyber-surveillance technologies at the multilateral level have come under increasing criticism. Several members of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (WA), most notably the United States, are concerned about unintended capture and harmful effects on computer security research.

The next few months will see important developments in the area of export controls on cyber-surveillance technologies. By discussing the control challenge and summarizing the perceptions and proposals of different participants in the debate, this article hopes to inform the ongoing policy debates. It will provide an overview of current developments on the European level and within the WA and present the current state of export controls on cyber-surveillance technology

---

2 A recent report by Ecorys and the Stockholm International Peace Research Institute (SIPRI) collected information on over 80 cases where cyber surveillance systems exported from the EU have been connected with violations of human rights or threats to international or EU security. See: "Final Report: Data and Information Collection for EU Dual-Use Export Control Policy Review," Ecorys and SIPRI , 2015, <https://www.sipri.org/sites/default/files/final-report-eu-dualuse-review.pdf>.

3 EU Commission, "Proposal for a Regulation of the European Parliament and of the Council Setting Up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (recast)," COM(2016) 616 final, Brussels, 2016, <http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154976.pdf>.

4 The INTA nominated MEP Klaus Buchner as Rapporteur. In parallel, the Committee on Foreign Affairs (AFET) will prepare an opinion on the proposal.

5 European Parliament, "Public Hearing Dual-Use Reform: How to 'future-Proof' EU Export Controls?," 2017, <https://polcms.secure.europarl.europa.eu/cmsdata/115347/programme-dual-use-reform-hearing.pdf>.

as well as interactions across governance levels. The article will also evaluate the existing response to limit the proliferation of cyber surveillance systems on the WA level, present an analysis of the current debate regarding the problematic definition of "intrusion software," and offer insights into alternative proposals—specifically whether a definition should rely on data exfiltration and user permission. The article discusses the outcome of the EU export control policy review, focusing on the regulation proposed by the Commission in September 2016 and provides an initial assessment of the key innovations and limitations of the draft text. The conclusion summarizes important findings and offers a brief outlook.

The Wassenaar Arrangement and its Discontents

Political Rationale for and Scope of the 2013 WA Amendments

The growing market for cyber-surveillance technologies entered into the spotlight following the 2011 Arab uprisings, when governments heightened the monitoring and censorship of communications in the region and the archives of deposed Arab regimes opened to the public.[6] In reaction to these revelations, legislative bodies in both the EU and the US have called for increased restrictions on cyber-surveillance and censorship technologies. In December 2013, the WA Plenary ratified two separate proposals from the UK and France to implement export controls related to 'intrusion software' and IP network surveillance systems. These amendments represented the recognition of an increasing need by the 41 participating governments to limit the proliferation of sensitive surveillance technologies to bad faith actors. The WA publishes two lists of controlled items which are not legally binding and are periodically reviewed and implemented based on national discretion. The decision to deny transfer of any item is the sole responsibility of each participating state.

The cyber-surveillance industry is comprised of a diverse set of companies of different sizes and degrees of specialization where the contours of the sector are not clearly defined. While a report by Ecorys and SIPRI estimates "over 250" active producers in Europe, a group of NGOs that formed the Coalition Against Unlawful Surveillance Exports (CAUSE) identifies 182 companies, and a recent effort by European journalists counted 235 "spy tech vendors headquartered in Europe."[7,8,9] This contains both companies, including many small enterprises, engaged exclusively in the development, production or export of cyber-surveillance

---

6 Among many individual reports, two major US news outlets and several civil society groups and international NGOs defending privacy and human rights, such as Privacy International, started to investigate the trade in cyber surveillance technologies more closely. See: "Wired for Repression," *Bloomberg*, 2011, <http://topics.bloomberg.com/wired-for-repression/>; "The Surveillance Catalogue," *Wall Street Journal*, 2011, <http://graphics.wsj.com/surveillance-catalog/#/>.

7 "Final Report: Data and Information Collection for EU Dual-Use Export Control Policy Review," Ecorys and SIPRI, 2015, <https://www.sipri.org/sites/default/files/final-report-eu-dualuse-review.pdf>.

8 "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," CAUSE, 2015, <https://privacyinternational.org/sites/default/files/CAUSE report v7.pdf>.

9 Maaike Goslinga and Dimitri Tokmetzis, "The Surveillance Industry Still Sells to Repressive Regimes. Here's What Europe Can Do about It," *The Correspondent*, 2017, <https://thecorrespondent.com/6249/the-surveillance-industry-still-sells-to-repressive-regimes-heres-what-europe-can-do-about-it/679999251459-591290a5>.

technologies and larger defense companies that provide a broad spectrum of cyber and non-cyber surveillance, and security solutions. Additionally, many ICT companies and technology giants produce technologies like probes, deep packet inspection, data storage, or analytics systems for both surveillance and non-surveillance end-uses. Because the sector is characterized by a high level of cross-border cooperation, the delivery of customized and integrated solutions, and the presence of a wide-range of specialized brokers and suppliers, the implementation of comprehensive controls is difficult and demanding for both licensing authorities and exporters.

The adoption of the first controls on cyber-surveillance technologies in 2013 set a precedent by introducing human rights considerations into the WA.[10] WA Member States, staying within the arrangement's narrow mandate, justified the measures arguing that these technologies, "under certain conditions, may be detrimental to international and regional security and stability."[11] According to the "Initial Elements" or foundational document of the WA, the organization shall "contribute(s) to international and regional peace and security" and does not include considerations relating to the internal affairs of states.[12] The French and UK governments—which had been heavily criticized by human rights activists for the export of surveillance technologies to authoritarian governments—were particularly interested in increasing their leverage over specific companies' export decisions. The UK government was concerned about the export of FinFisher intrusion technologies by Gamma International, a British-German company. The French government proposed the restriction on IP network surveillance systems after evidence emerged that Amesys, a French company, supplied its monitoring system to Libya under Gaddafi, where it was "deployed against dissidents, human-rights campaigners, journalists or everyday enemies of the state."[13,14] France implemented the control almost immediately after it was approved by the WA, leaving EU members behind.[15]

Neither amendment was designed to solve the totality of threats to privacy and human rights stemming from cyber-surveillance technologies, but they represented the first important steps

---

10 "Comment Submitted by Privacy International in Response to the Proposed Rule (RIN 0694-AG49) Implementing Controls on Intrusion and Surveillance Items Agreed within the Wassenaar Arrangement in 2013," Privacy International, 2015, <https://privacyinternational.org/sites/default/files/Privacy International BIS submission.pdf>; and Tim Maurer, "Internet Freedom and Export Controls," Carnegie, 2016, <http://carnegieendowment.org/2016/03/03/internet-freedom-and-export-controls/iutd>.

11 "Public Statement 2013 Plenary Meeting of The Wassenaar Arrangement On Export Controls for Conventional Arms And Dual-Use Goods And Technologies," Wassenaar Arrangement Secretariat, 2013, <http://www.wassenaar.org/wp-content/uploads/2015/06/WA-Plenary-Public-Statement-2013.pdf>.

12 "Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies," Wassenaar Arrangement Secretariat, 2014, <http://www.wassenaar.org/wp-content/uploads/2015/06/Guidelines-and-procedures-including-the-Initial-Elements.pdf>.

13 "British Government Admits It Started Controlling Exports of Gamma International's FinSpy," Citizen Lab, 2012, <https://citizenlab.org/2012/09/british-government-admits-it-started-controlling-exports-of-gamma-internationals-finspy/>; "Reports from the Business, Innovation and Skills, Defence, Foreign Affairs and International Development Committees Session 2013-14 Strategic," UK Government, 2013, p. 37, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/264089/8707.pdf>.

14 Margaret Coker and Paul Sonne, "Life Under the Gaze of Gadhafi's Spies," *The Wall Street Journal*, 2011, <http://www.wsj.com/news/articles/SB10001424052970203764804577056230832805896>.

15 "Comment Submitted by Privacy International in Response to the Proposed Rule (RIN 0694-AG49) Implementing Controls on Intrusion and Surveillance Items Agreed within the Wassenaar Arrangement in 2013," Privacy International, 2015, <https://privacyinternational.org/sites/default/files/Privacy International BIS submission.pdf>.

towards imposing controls on the multilateral level. The coverage of both categories has raised some concerns with a broad range of actors and implementation of the amendments remains uneven; to date, the US has not implemented the controls.[16] The category on IP network surveillance, which covers systems that conduct high performance analysis of internet traffic, is criticized for its scope because it appears extremely narrow – and as a result risks failing to catch some of the systems that are of most concern.[17] On the other hand, the control on intrusion software came under intense criticism because it employs overly broad definitions.

Instead of adding intrusion software directly to the control list, the WA establishes a definition of "intrusion software" and derives from this a second group of items that is placed under export controls. This two-tier structure leads to the restriction of the command and control infrastructure used to generate, install, and instruct the spyware, i.e., the components that stay with the purchaser, not any component that would end up on a victim's device. Although this delineation was put in place to protect targeted users and IT security businesses, cybersecurity researchers, and multinational companies have raised significant concerns. Especially in the US, implementation met stiff resistance.[18] Several security researchers have asserted that "contrary to the WA's standards, these entries are defined by pseudo-technical language, the possible interpretations of which are manifold."[19] They worry that the definition of intrusion software applies "almost universally to the building blocks of security research," which could have "chilling effects on the development of anti-surveillance measures and on the discovery of existing vulnerabilities."[20]

---

16 The European Union adopted the provisions in October 2014, see: Council Regulation (EC) No. 428/2009 of 5 May 2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items, Official Journal of the European Union (L 134/1) of May 29, 2009. It is unlikely that the provisions will be fully implemented in the US. The Bureau of Industry and Security retracted the implementing regulation following a comment period in which it "received more than 260 comments, virtually all of them negative." See: "Wassenaar: Cybersecurity and Export Control," United States Congress, 2016, <https://oversight.house.gov/hearing/wassenaar-cybersecurity-and-export-control/>.

17 The interception of these communications, including online searches, emails, and VoIP calls, lies at the heart of many mass surveillance systems. Because the listing specifies an extensive set of capabilities, which systems need to offer in order to fall under this export restriction, the WA language on IP network surveillance remains extremely narrow and does not cover the broad spectrum of network technologies that could be employed for repressive purposes. See Collin Anderson, "Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies," Access, 2015, <https://cda.io/r/ConsiderationsonWassenaarArrangementProposalsforSurveillanceTechnologies.pdf>; and Tim Maurer, Edin Omanovic, and Ben Wagner, "Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age," New America Foundation, Open Technology Institute, March 2014, <https://cihr.eu/wp-content/uploads/2014/06/Uncontrolled-Surveillance_March-2014.pdf>.

18 Katie Moussouris, "You Need to Speak Up For Internet Security. Right Now," *Wired*, 2015, <http://www.wired.com/2015/07/moussouris-wassenaar-open-comment-period/>; Kim Zetter, "Why an Arms Control Pact Has Security Experts Up in Arms," *Wired*, 2015, <http://www.wired.com/2015/06/arms-control-pact-security-experts-arms/>.

19 Thomas Dullien, Vincenzo Iozzo, and Mara Tam, "Surveillance, Software, Security, and Export Controls. Reflections and Recommendations for the Wassenaar Arrangement Licensing and Enforcement Officers Meeting," 2016, <https://drive.google.com/file/d/0B5hBKwgSgYFaN2xHUkdIYWN2Mnc/view>; Sergey Bratus et al., "Why Offensive Security Needs Engineering Textbooks," Dartmouth University, 2014, <http://www.cs.dartmouth.edu/~sergey/drafts/why-offensive-security-needs-textbooks.pdf>.

20 Sergey Bratus et al., "Why Wassenaar Arrangement's Definitions of Intrusion Software and Controlled Items Put Security Research and Defense At Risk — And How To Fix It," Dartmouth University 2014, pp. 1–13.

Avoiding Unintended Capture

Striking the right balance between benefits and costs is a common challenge across all export control categories for dual-use items. Unduly stringent or ill-defined controls on cyber-surveillance technologies can hurt legitimate business interests and have harmful effects on computer security research. Definitions and control lists need to provide clear guidance for companies and for national licensing authorities that encourages consistency in implementation between Member States—an issue that is also highly relevant in the context of the EU reform proposal. For many observers, the current mechanism of capture of the WA controls and its implementation on the EU level does not produce efficient controls. IT security researchers and companies have argued that the complete removal or renegotiation of the 2013 amendments is preferable to their (partial) adoption, which would make the provisions subject to divergent national interpretation.[21] NGOs, privacy and human rights activists, and other researchers, however, oppose calls for the elimination and argue for clarifications, specific exemptions, controls that apply only to end use cases and end-users facilitating or conducting surveillance, as well as clearer definitions for the most contentious categories.[22]

The core problem is that the existing WA entries on "intrusion software" (Categories 4.A.5., 4.D.4., 4.E.1.a., and 4.E.1.c.) are based on technical attributes common to both commercial surveillance and information security tools—those technologies to infiltrate targeted devices without consent and those for testing for vulnerabilities. IT security researchers emphasize that "it is impossible to distinguish among malicious and innocuous software on a technical basis" and some even argue that "unless a specific software can be confidently classified as "single-use," it would be highly unwise to regulate it."[23,24] A number of alternative proposals suggest focusing on the critical dependence of surveillance software "to secretly exfiltrate data from the computer, without user permission or knowledge" to ensure that legitimate research and

---

21 Dullien, Iozzo, and Tam, "Surveillance, Software, Security, and Export Controls. Reflections and Recommendations for the Wassenaar Arrangement Licensing and Enforcement Officers Meeting;" and Microsoft Corporation, "Written Testimony of Cristin Flynn Goodwin Assistant General Counsel for Cybersecurity at Microsoft Corporation; Joint Subcommittee Hearing on Wassenaar: Cybersecurity & Export Control January 12, 2016," United States Congress, 2016, <https://oversight.house.gov/wp-content/uploads/2016/01/Goodwin-Microsoft-Statement-1-12-Wassenaar.pdf>; Cheri F . McGuire, "Prepared Testimony and Statement for the Record of Cheri F. McGuire Vice President, Global Government Affairs & Cybersecurity Policy; Symantec Corporation Hearing on Wassenaar: Cybersecurity & Export Control Before the House Committee on Homeland," United States Congress, 2016, <https://oversight.house.gov/wp-content/uploads/2016/01/McGuire-Symantec-Statement-1-12-Wassenaar.pdf>.

22 Access et al., "Comments to the US Department of Commerce on Implementation of 2013 Wassenaar Arrangement Plenary Agreements (RIN 0694-AG49)," 2015, <https://www.eff.org/files/2015/07/21/jointwassenaarcomments-final-1.pdf>; and Electronic Frontier Foundation, "Comments of the Electronic Frontier Foundation on the Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, RIN 0694-AG49," 2015, <https://www.eff.org/files/2015/07/21/effwassenaarcomments-1.pdf>.

23 Dullien, Iozzo, and Tam, "Surveillance, Software, Security, and Export Controls. Reflections and Recommendations for the Wassenaar Arrangement Licensing and Enforcement Officers Meeting," WA-CAT4 Draft, 2015, <https://tac.bis.doc.gov/index.php/documents/pdfs/299-surveillance-software-security-and-export-controls-mara-tam/file>.

24 Vincenzo Iozzo, "Speech to Members of the European Parliament and European Commission, September 30, 2015," 2015, <https://drive.google.com/file/d/0B3NL8jkEQKjYcnp5aUtsSVRoQjA/view?pref=2&pli=1>.

information sharing is still possible without the need to apply for an export license.[25] Because "the vast majority of exfiltration software has no legitimate use," it "could safely be regulated without having adverse consequences on legitimate security research."[26]

Some proposals also call for a control approach that "takes into account the intent of the technology and software developer."[27] By shifting the definition of "intrusion software" to focus on intent, not functionality, the export authorization would rely more on contextual information. Manifest intent could, for example, be established by looking at the way the software is designed, i.e., whether it is designed to be used against a non-consenting other party, or the way the software is marketed.[28] This approach tries to reconcile both sides of the debate by adding to the definition of intrusion software the criterion of authorization by the owner of the targeted device to install software or perform specific actions.[29]

However, while the overlap between offensive and defensive applications seems to necessitate increased attention to the intended use of technologies, it also complicates the export authorization process.[30] Because export controls are critically dependent on the capacity to define an item with legal precision in a manner that can be employed at some stage prior to the transfer, categories on the dual-use list are traditionally based on precisely defined performance metrics. While it might be possible to identify certain products by relying on user authorization as a criterion, this would not apply to the full spectrum of relevant technologies. Similarly, a definition of intrusion software dependent on its intended use would likely pose a higher administrative burden for licensing authorities, while exporters would be required to provide additional information on customers and develop further so-called "know your customer approaches." The ambiguity of a classification of products based on intent may also be compounded by the component nature of cyber-surveillance systems; licensing authorities would need additional technical expertise to identify critical exports.

---

25 Sergey Bratus et al., "Why Offensive Security Needs Engineering Textbooks," Dartmouth University, 2014, <http://www.cs.dartmouth.edu/~sergey/drafts/why-offensive-security-needs-textbooks.pdf>.

26 Vincenzo Iozzo, "Speech to Members of the European Parliament and European Commission, September 30, 2015," 2015, <https://drive.google.com/file/d/0B3NL8jkEQKjYcnp5aUtsSVRoQjA/view?pref=2&pli=1>.

27 "Comment Submitted by Privacy International in Response to the Proposed Rule (RIN 0694-AG49) Implementing Controls on Intrusion and Surveillance Items Agreed within the Wassenaar Arrangement in 2013," Privacy International, 2015, <https://privacyinternational.org/sites/default/files/Privacy International BIS submission.pdf>; "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," CAUSE Report, June 2015, p. 17, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>.

28 Thomas Dullien, "An Attempt at Fixing Wassenaar," ADD/XOR/LOR Blog, 2016, <http://addxorrol.blogspot.de/>.

29 Dullien, Iozzo, and Tam, "Surveillance, Software, Security, and Export Controls. Reflections and Recommendations for the Wassenaar Arrangement Licensing and Enforcement Officers Meeting," WA-CAT4 Draft, 2015, <https://tac.bis.doc.gov/index.php/documents/pdfs/299-surveillance-software-security-and-export-controls-mara-tam/file>.

30 This can also be highlighted with reference to the Tallinn Manual on the International Law Applicable to Cyber Warfare, which defines a 'cyber weapon' by the effects it may have, rather than by its nature or components, or means of operation or construction. (See Tallinn Manual Rule 41 No 2).

Avenues for Future Activity on the WA Level

Revising the relevant WA language has proven difficult, not least because the majority of the 41 members have already implemented the provisions, and the controls on cyber-surveillance technologies are only two of many items to be reviewed and discussed.[31] On March 1, 2016, the US government sent an open letter to several business associations in which it explained that the administration "has proposed in this year's WA [review] to eliminate the controls on technology required for the development of 'intrusion software.'"[32] After some initial successes in mid-2016, when the parties agreed in principle to clarify some of the wording and asked for a report detailing specific examples of cybersecurity tools that might be inappropriately covered, the WA Plenary of December 2016 failed to rephrase the most important provisions with regard to vulnerability research and disclosure.[33] Despite the US government's two-year effort, delegates could not reach a unanimous decision to ease the export restrictions, which shows the difficulties inherent in the multilateral negotiation process.[34] It will now be up to the new US Trump administration to decide whether to continue renegotiations.[35]

The difficulties encountered when trying to modify the arrangement's existing provisions also give some indication of the challenges in creating multilateral controls for additional products and services—which remains the preferred course of action for many stakeholders, including European exporters of cyber-surveillance technologies.[36] Export controls should principally be established on the highest possible level to increase their impact and prevent circumvention. Further attempts to add cyber-surveillance technologies to the WA on human

---

31 Tim Maurer, "Internet Freedom and Export Control," Carnegie Endowment for International Peace, 2016, <http://carnegieendowment.org/2016/03/03/internet-freedom-and-export-controls-pub-62961>.

32 "Letter from Secretary Pritzker to Several Associations on the Implementation of the Wassenaar Arrangement 'intrusion Software' and Surveillance Technology Provisions," US Department of Commerce, March 1 2016, 2016, <https://www.bis.doc.gov/index.php/oee/9-bis/carousel/1010-letter-from-secretary-pritzker-to-several-associations-on-the-implementation-of-the-wassenaar-arrangement-intrusion-software-and-surveillance-technology-provisions>; "Major Business and Tech Groups Call on Administration Officials to Renegotiate Wassenaar Arrangement to Strengthen Cybersecurity," Information Technology Industry Council, 2016, <http://www.itic.org/dotAsset/9/8/98c27c3a-609b-41e3-8f7b-4fe1bb642ad6.pdf>.

33 With regard to categories 4.A.5., 4.D.4, the definition of 'intrusion software' was amended. See page 215 of the WA Dual-use List: <http://www.wassenaar.org/wp-content/uploads/2016/12/WA-LIST-16-1-2016-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf>;

34 Iain Mulholland and Katie Moussouris, "Administration Should Continue to Seek Changes to International Cyber Export Controls," *The Hill*, 2017, <http://thehill.com/blogs/congress-blog/technology/316978-administration-should-continue-to-seek-changes-to>; Iain Thomson, "Wassenaar Weapons Pact Talks Collapse Leaving Software Exploit Exports in Limbo," *The Register*, 2016, <http://www.theregister.co.uk/2016/12/21/wassenar_negotiations_fail/>.

35 Jim Langevin, "Langevin Statement on Wassenaar Arrangement Plenary Session," Congressman Jim Langevin Website, December 19, 2016, <http://langevin.house.gov/press-release/langevin-statement-wassenaar-arrangement-plenary-session>.

36 See for example the statements of expert witnesses from industry associations and producers at the European Parliament, "Recording of the INTA Public Hearing on the Reform of the EU Dual-Use Legislation," March 21, 2017, <http://www.europarl.europa.eu/news/en/news-room/20170316IPR67192/committee-on-international-trade-21032017-(pm)>.

rights grounds will, however, likely meet significant resistance.[37] The WA's traditional focus on conventional arms and dual-use items for the production of Weapons of Mass Destruction WMDs) places significant limits on the types of surveillance technologies that can be added. The present controversy about unintended capture, the business-friendly attitude of the new US administration, and generally diverse WA membership, which, for example, includes Russia and remains subject to EU and US sanctions—are also likely to increase opposition.

Given the inefficiency of controls and the lack of progress on the multilateral level, EU Member States have—in some cases reluctantly—developed further the European control regime and independently implemented additional controls on the national level.[38] For example, Italy established restrictions in 2012 following reports that an Italian company had begun to install a monitoring center in Syria.[39] More recently, the German government introduced national controls on items that are not listed at the WA or EU level in July 2015 after a German proposal to add additional lawful interception technologies to the WA lists did not gain traction from late 2014 to early 2015.[40] Germany argued that national measures had become necessary because similar restrictions on the European level "could not be expected before 2017" but would repeal the national controls once a European solution had been implemented.[41] On the European level, an increasing number of actors, including a majority of the European Parliament, have argued for an independent mechanisms through which to control the export of cyber-surveillance technologies. The draft regulation on dual-use exports recently published by the European Commission, which will be discussed in the next section, represents an important step in this direction and takes up many suggestions made in the debate and public consultation.

---

37 Ian J. Stewart and Sibylle Bauer, *Workshop: Dual-Use Export Controls (Background Paper)*, 2015, p. 30, <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/535000/EXPO_STU(2015)535000_EN.pdf>.

38 Article 8 (1) of Regulation 428/2009 permits EU governments to impose national controls on non-listed items for reasons of public security or human rights considerations. This clause has repeatedly been used to control cyber surveillance technologies.

39 The company in question, Area S.p.A., announced that it would not complete the installation of the monitoring center. See Vernon Silver, "Italian Firm Exits Syrian Monitoring Project, Repubblica Says," *Bloomberg Business*, 2011, <http://www.bloomberg.com/news/articles/2011-11-28/italian-firm-exits-syrian-monitoring-project-repubblica-says>; Italian Government, "Notices From Member States Regarding Council Regulation (EC) No 428/2009: Regarding Delivery of Monitoring System to Syria," 2012, <http://trade.ec.europa.eu/doclib/docs/2012/september/tradoc_149946.pdf>.

40 The fourth amendment to the German Foreign Trade Ordinance establishes new control list categories covering monitoring centers and data retention systems and introduces authorization requirements on the provision of 'technical assistance,' an intentionally broad concept of related services. However, the national controls affect only a small number of companies, many of which had already been subject to export controls on encryption technologies. See: Stephanie Horth, Joanna Bronowicka, and Ben Wagner, "Policy Brief Export Control," Centre for Internet and Human Rights, 2015, <https://cihr.eu/export-controls-policy-paper/>.

41 German Government, *Vierte Verordnung zur Änderung der Außenwirtschaftsverordnung*, 2015, <https://www.bmwi.de/BMWi/Redaktion/PDF/V/vierte-verordnung-zur-aenderung-der-aussenwirtschaftsverordnung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf>.

EU Dual-Use Export Controls and Policy Review

The Outcome of the Export Control Policy Review

Increasing exports of cyber-surveillance technologies have been addressed by the European Union through a series of loosely connected measures. These include the broadening of specific sanction regimes from 2011 onwards, the implementation of WA amendments in October 2014, the adoption of human rights guidelines with regard to freedom of expression online, and a wide-ranging review of the EU's dual-use export control policies.[42] This section analyzes the outcome of the export control policy review, which was broadly aimed at updating the regulatory framework on dual-use exports, regulatory simplification, and "an initiative to control ICTs to prevent violations of human rights and protect the EU's security."[43]

On September 28, 2016, the European Commission proposed a draft regulation to modernize the existing control regime, highlighting the need for "adjusting to evolving security risks and threats; adapting to rapid technological and scientific developments; [and] preventing the export of cyber-surveillance technology in violation of human rights."[44] The Commission characterized the proposal as an ambitious step that combines elements of a more pragmatic export control "system update" aimed at adjusting the existing framework with a forward-looking "system modernization" focusing on cyber-surveillance technologies and human rights.[45] The draft would replace Regulation 428/2009, adopted in May 2009, which so far formed the basis for the EU's common policy on export controls for dual-use items, including cyber-surveillance technologies. The Dual-Use Regulation establishes rules for export, transit, brokering, and intra-community transfer procedures across EU Member States and aggregates externally-originating requirements that are agreed within the WA and other multilateral export control regimes. The regulation is binding and directly applicable throughout the EU but leaves implementation and enforcement to Member States, including decisions regarding whether to grant or to refuse export licenses—although coordination measures exist to promote uniform implementation.[46]

---

42 Following revelations about European companies selling surveillance technologies to Iran and Syria, country-specific sanctions regimes were updated as part of the EU's Common Foreign and Security Policy (CFSP). In December 2011, a broad ban on equipment and software "for use in the monitoring or interception by the Syrian regime, or on its behalf, of the internet and of telephone communications on mobile or fixed networks" and the provision of associated services was added to sanctions against Syria. In March 2012, equivalent language was inserted into the Iran embargo.

43 "Roadmap. Review of the EU Dual-Use Export Control Regime," European Commission, 2015, <http://ec.europa.eu/smart-regulation/impact/planned_ia/docs/2015_trade_027_duxc_en.pdf>; and "Green Paper: The Dual-Use Export Control System of the European Union: Ensuring Security and Competitiveness in a Changing World," European Commission, 2011, <http://trade.ec.europa.eu/doclib/docs/2011/june/tradoc_148020.pdf>.

44 "Report on the EU Export Control Policy Review - Executive Summary of the Impact Assessment (Accompanying the Proposal)," European Commission, 2016, <http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154978.pdf>.

45 These terms describe Policy Option 3 and Option 4 set out in the Roadmap for the export control policy review, cf. European Commission, "Roadmap. Review of the EU Dual-Use Export Control Regime."

46 To avoid delays, the Commission has delegated authority to update the control list pursuant to regulation 599/2014. At the time of writing, the latest version of the control list is regulation 2016/1969 of 12 September 2016.

The proposed regulation places significant emphasis on the control of cyber-surveillance technologies. The official impact assessment for the regulation argues that a modernization of the existing regime "appears indispensable to achieve the objective to prevent human rights violation caused by the lack of appropriate controls of cyber-surveillance technology."[47] To this end, the definition of dual-use items has been revised in Article 2.1b of the draft to specifically include "cyber-surveillance technology which can be used for the commission of serious violations of human rights or international humanitarian law, or can pose a threat to international security or the essential security interests of the Union and its Member States." Taking up and combining some of the initial proposals in the review, the draft regulation sets out a twofold control approach: first, it introduces an EU autonomous control list of specific cyber-surveillance technologies (Annex 1B "List of Other Dual-Use Items).[48] Second, it establishes a targeted catch-all clause designed to act as an emergency brake in cases "where there is evidence that the items may be misused by the proposed end-user for directing or implementing serious violations of human rights or international humanitarian law in situations of armed conflict or internal repression in the country of final destination."[49]

The new regulation also for the first time features a definition of cyber-surveillance technology which is broadly understood as "items specially designed to enable the covert intrusion into information and telecommunication systems with a view to monitoring, extracting, collecting and analyzing data, and/or incapacitating or damaging the targeted system."[50] This constitutes a wide definition of the technologies in question and is developed further by explicitly stating that "[t]his includes items related to the following technology and equipment: mobile telecommunication interception equipment; intrusion software; monitoring centers; lawful interception systems and data retention systems; digital forensics."[51] Interestingly, the definition has been narrowed between July 2016, when a draft of the proposal was leaked, and the official publication in September 2016.[52] While the old definition reflected the very broad conception of cyber-surveillance technologies available in the Ecorys/SIPRI report supporting the EU impact assessment, the new version no longer explicitly refer to biometrics, location tracking,

47 "Report on the EU Export Control Policy Review - Executive Summary of the Impact Assessment (Accompanying the Proposal)," European Commission, 2016, <http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154978.pdf>.

48 Green Paper: The Dual-use Export Control System of the European Union: Ensuring Security and Competitiveness in a Changing World," DG Trade, European Commission, 2011, <http://trade.ec.europa.eu/doclib/docs/2011/june/tradoc_148020.pdf>, p. 2.

49 "Report on the EU Export Control Policy Review - Executive Summary of the Impact Assessment (Accompanying the Proposal)," European Commission, 2016, <http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154978.pdf>.

50 See Article 2.2.21 of the draft regulation.

51 Ibid.

52 Catherine Stupp, "Commission Plans Export Controls for Surveillance Technology," *Euractiv*, 2016, <https://www.euractiv.com/section/trade-society/news/technology-companies-face-export-hurdles-under-draft-eu-rules/>.

probes, and deep packet inspection systems.[53,54] The accompanying documents did not explain the rationale behind the clarification; it might be due to concerns regarding unintended capture and administrative costs for national agencies or exporters. This will be discussed in the next sections, which introduce key innovations in the proposal and offer an assessment of the wider implications and limitations of the draft text so far as it relates to cyber-surveillance technologies.

An EU Autonomous Control List: Additional Coverage but a Lack of Clarity

The Commission has proposed to introduce an EU autonomous list with the aim to control the export of specific items necessary in cyber-surveillance that are not part of other applicable control lists.[55] This represents an important and ambitious step that has also been advocated by different actors in the debate.[56] However, EU governments and industry have previously sought to avoid adopting EU-level controls on items that are not included on the WA level due to concerns about implementation costs and the competitiveness of EU-based companies. The Commission has therefore been very careful to highlight that the new control measures "should not go beyond what is proportionate" and the impact assessment states, "[t]he precise design of those new controls would ensure that negative economic impact will be strictly limited and will only affect a very small trade volume."[57] Reliable estimates regarding the size of the cyber-surveillance sector are, of course, hard to come by, but SIPRI recently conducted a trade analysis of dual-use related exports of ICT goods. They found dual-use related exports in electronics of €31.7 billion, in computers of at least €2 billion, and in telecommunications and 'information security' of up to €22.6 billion for the year 2014.[58] Still, it remains impossible to infer from these figures the export volume of especially critical technologies like intrusion software, which accounts only for a small percentage of these figures.[59] Further taking into account that these numbers represent global exports, it is likely that the new controls will only affect a small amount of this trade, which can be reduced further by defining the controlled technologies and circumstances in which export authorization should be denied more accurately.

---

53 Ecorys and SIPRI, "Final Report: Data and Information Collection for EU Dual-Use Export Control Policy Review," 2015, pp. 147-9, 218.

54 Civil society actors such as a group of NGOs represented by the Coalition Against Unlawful Surveillance Exports (CAUSE) have argued for additional controls on voice identification technology, location monitoring technology and additional systems for collecting data as it passes through communications networks (LI solutions and 'inter-connectors', probes and fiber taps). Most of these would have been part of the definition of cyber-surveillance technology in the version as of July 2016. See "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," CAUSE, 2015, <https://privacyinternational.org/sites/default/files/CAUSE report v7.pdf>.

55 Regulation 428/2009 aggregates externally-originating requirements that are agreed within other forums, specifically the WA, the Missile Technology Control Regime, the Nuclear Suppliers' Group, the Australia Group and the Chemical Weapons Convention.

56 Green Paper: The Dual-use Export Control System of the European Union: Ensuring Security and Competitiveness in a Changing World," DG Trade, European Commission, 2011, <http://trade.ec.europa.eu/doclib/docs/2011/june/tradoc_148020.pdf>, p. 2.

57 See recital (5) of the draft EU regulation.

58 Based on Eurostat data and mirroring the ECCN categories 3 to 5. Ecorys and SIPRI, "Final Report: Data and Information Collection for EU Dual-Use Export Control Policy Review," 2015, p. 146.

59 This can be inferred from looking at national export statistics on cyber-surveillance technologies that is made publicly available by the UK and Switzerland.

Although the coverage of the proposed autonomous list remains limited, few countries seem to support the approach.[60] A 2015 survey by Ecorys and SIPRI of Member State governments found that only a small number of respondents are in favor of controlling additional technologies such as "LI systems, data retention systems, and covert mass surveillance."[61] Interestingly, the new Annex 1B mirrors the control provisions that were implemented by the German government on the national level with regard to Law Enforcement Monitoring Facilities and data retention systems in July 2015.[62] However, a group of EU Member States, including Germany, France, and the UK, asked the Commission before publication of the proposal to scrap the autonomous list approach, allegedly arguing that "unilateral EU lists would be less effective, [and] undermine the competitiveness of EU industry."[63] Instead, they proposed to attempt further negotiations on the WA level or in an alternative international setting beyond the EU, a shift that would further delay the establishment of effective controls for cyber-surveillance technologies. This would, of course, significantly decrease the impact and innovative character of the new EU regulation.

Unilateral, EU-wide controls have especially been opposed by the European cyber-surveillance industry but also have effects beyond Europe. Press reports indicate that the Commission has been approached by companies and industry associations fearing that the regulation would decrease their competitiveness and legal certainty, and could even force companies to move outside the EU.[64] A group of Commissioners, led by then-Commissioner for Digital Economy Günther Oettinger, allegedly argued for a more business-friendly regulation and lobbying efforts might already have led to the narrowing of the definition of cyber-

60 Section B of Annex I ("Other Items of Cyber-Surveillance Technology" contains entries for monitoring centers for lawful interception and data retention systems or parts thereof (10A001) as well as the respective provisions on the software (10D001) and technology (10E001) necessary for the items specified in 10A001. The new controls may offer a potential loophole because, according to the technical note, category 10A001 includes an exemption for products designed for and used at telecommunications companies (service providers). Especially data retention is often performed by service providers and in many authoritarian states these have close ties to the state. This exemption has already been criticized in the context of the German controls; the impact on the effectiveness of the controls remains, however, difficult to assess. See for example Catherine Stupp, "Germany Leaves Brussels behind on Surveillance Tech Export Controls," *Euractiv*, 2015, <http://www.euractiv.com/section/digital/news/germany-leaves-brussels-behind-on-surveillance-tech-export-controls/>.

61 Ecorys and SIPRI, "Final Report: Data and Information Collection for EU Dual-Use Export Control Policy Review," 2015, pp. 147-9, 218.

62 This relates to the German Foreign Trade Ordinance (*Außenwirtschaftsverordnung*) and especially the categories 5A902, 5D902, 5E902 in Appendix 1 (AL) Part I B (in force 18.07.2015).

63 EurActiv reported that Austrian, Finnish, French, German, Polish, Slovenian, Spanish, Swedish, and UK diplomats circulated a memo asking the Commission to scrap the list of products that will be subject to EU export controls and instead broker an international agreement that involves countries outside the EU. See: Catherine Stupp, "Tech Industry, Privacy Advocates Pressure Commission on Export Control Bill," *Euractiv*, 2016, <https://www.euractiv.com/section/trade-society/news/tech-industry-privacy-advocates-pressure-commission-on-export-control-bill/>.

64 Because the sector is highly fragmented and companies offer a very heterogeneous set of goods, services and technologies, they are not represented by a single industry association. Rather, certain companies are members of ICT-focused associations, such as Digital Europe, or IT-focused associations, such as BitKom, or defense and security associations, such as ASD, while especially smaller companies are not members of any association.

surveillance technology described above.[65] In terms of implementation, the Commission's impact assessment concedes that controls on cyber-surveillance technologies "could result in a higher administrative burden for operators and authorities, since a new category of goods and technology would be subject to control."[66] In addition, it has been argued that an autonomous list could generate some confusion with non-EU states that refer to the EU dual-use list as a synthesis of multilateral regimes that are nationally implemented.[67] Would the EU start to include additional technologies because of specific human rights concerns, these countries might stop aligning their national control lists with the EU framework, thus decreasing the indirect influence of the EU on export controls globally. On the other hand, unilateral measures—together with some active diplomacy—could also allow the EU to demonstrate how cyber-surveillance technologies can effectively be controlled and increase the chances that others might follow or enact similar controls.

Much work is still required to ensure that legitimate exports are not inadvertently caught. The proposal offers some assurances that the new controls do "not prevent the export of information and communication technology used for legitimate purposes, including law enforcement and internet security research."[68] While the Commission intends to develop guidelines to support the practical application of the proposed controls, it recently described the development of these guidelines as a principally "operational issue" that could be addressed later. For all affected communities, the vagueness of the new control provisions on cyber-surveillance technologies remains a key concern. The lack of clarity on what, for example, can be classified as "digital forensics," a term used in the proposal's definition of cyber-surveillance technology, in combination with the new catch-all provision, has been raised by companies and NGOs alike. Privacy International rightly observes that "like intrusion software, forensic tools can be used to enhance and improve cybersecurity, and by extension protect human rights globally, and must not be restricted when moving between international parties to remedy problems with IT systems."[69] The discussion on the coverage of the proposed regulation thus mirrors the situation on the WA level, where a lack of clear definitions creates legal uncertainty and inconsistent implementation.

An important question also is whether the Commission would be empowered to add technologies independently to the autonomous list (Annex 1 Section B), which is currently

---

65 Ibid.

66 "Report on the EU Export Control Policy Review - Executive Summary of the Impact Assessment (Accompanying the Proposal)," European Commission, September 28, 2016, <http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154978.pdf>.

67 Sibylle Bauer and Mark Bromley, "The Dual-Use Export Control Policy Review: Balancing Security, Trade and Academic Freedom in a Changing World," *Nonproliferation Papers* 48 (2016) p. 8, <http://www.nonproliferation.eu/web/documents/nonproliferationpapers/the-dual-use-export-control-policy-review-balancin-49.pdf>.

68 Preamble of the draft regulation, recital (5).

69 Edin Omanovic, "Landmark Changes to EU Surveillance Tech Export Policy Proposed, Leaked Document Shows," Privacy International, July 2016, <https://www.privacyinternational.org/node/909>.

envisioned in Article 16.2b of the draft.[70] Delegated acts were previously only used to aggregate externally-originating requirements negotiated by the Member States in multilateral export control forums. Article 16.2 would enable the Commission to assess the risks associated to non-listed technologies and to enact additional controls on cyber surveillance technologies if it proves necessary, an approach which has been suggested by some researchers.[71] It is likely that Member States would oppose this appreciation of the Commission's role and the lack of clear selection and assessment criteria for this process has already attracted criticism by national export licensing bodies.[72]

Overall, the proposal remains unclear in the details of what constitutes controlled cyber-surveillance technologies and more clarity is needed before all concerned stakeholders can fully understand the nature and functioning of these controls. Going forward, it will be crucial to work out and communicate the differences between the way in which exports of specific technologies aid in the violation of fundamental human rights and, alternatively, support legitimate IT security practices. There remains a considerable need for clarification and additional work on the control requirements at the European level and, for those Member States that seek to actively support the redrafting of the WA controls on intrusion software, a need for outreach efforts aimed at inviting affected and interested parties to provide expertise on how to implement the controls. On both levels, existing proposals to distinguish technology based on data exfiltration and user consent might certainly be worthy of further exploration.[73] Legal certainty is especially critical in the case of cyber-surveillance technologies because only clear-cut authorization requirements can act as a credible preventive and deterrent measure.

Strengthening the Role of Human Rights in the Export Authorization Process

Much of the discussion over the last years has focused on the way in which EU Member States address human rights considerations in their export licensing processes. By incorporating important innovations based on the human security approach, the Commission proposal represents a major step towards an explicit obligation for national licensing authorities to base their assessments on respect for human rights and the internal situation in the country of final destination. Going forward, it will, however, be necessary to clarify the language and obligations further and provide effective guidance or even clear criteria to the Member States specific to licensing assessments on cyber-surveillance technology.

While the inclusion of human rights considerations in licensing decisions on dual-use exports is already required under the EU dual-use regulation, Member States have interpreted and applied

---

70 According to Article 16.2b, the Commission would be empowered to adopt delegated acts to amend Section B of Annex I "if this is necessary due to risks that the export of such items may pose as regards the commission of serious violations of human rights or international humanitarian law or the essential security interests of the Union and its Member States."

71 Ian Stewart and Sibylle Bauer, "Workshop: Dual-Use Export Controls (Background Paper)," European Parliament, 2015, p. 30, <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/535000/EXPO_STU(2015)535000_EN.pdf>.

72 Statement by an expert of the Federal Office for Economic Affairs and Export Control, Germany, see: "Recording of the INTA Public Hearing on the Reform of the EU Dual-Use Legislation (March 21, 2017)," European Parliament, 2017.

73 See Section 2.2 above.

these criteria differently. Article 12 of the existing regulation requires Member States to base their decisions on the authorization of exports on all relevant considerations, "including those covered by Council Common Position (2008/944/CFSP) defining common rules governing control of exports of military technology and equipment." However, while the Common Position provides a basic set of criteria, the European Parliament has repeatedly criticized that it "is being applied loosely and interpreted inconsistently by the Member States," which is especially true for the criterion on human rights.[74,75] Consequently, there is a clear need to move closer towards agreed EU-wide standards that highlight the role of human rights in assessment processes for dual-use exports.

The proposed regulation puts in place a clear obligation for EU governments to assess human rights implications and deny applications where there is a clear risk of human rights abuses. The new Article 14, which is based on Article 12 of the existing regulation, states explicitly that competent authorities should consider "respect for human rights in the country of final destination as well as respect by that country of international humanitarian law" and "the internal situation in the country of final destination." This could considerably strengthen the role of human rights criteria in the assessment process and lead to a more uniform application of the existing assessment criteria across Member States. In addition, the regulatory intent becomes evident in the preamble to the proposed regulation, which "clarifie[s] that assessment criteria for the control of exports of dual-use items include considerations regarding their possible misuse in connection with acts of terrorism or human rights violations."[76]

The draft reflects the initial proposal by the Commission which aimed at evolving the existing regime "towards a 'human security' approach recognizing that security and human rights are inextricably interlinked."[77] This approach shifts attention from national security issues related to potential military end-uses to people-centered security, for example, terrorism and human rights violations, which becomes evident with the additional catch-all clauses in Article IV.[78] The additions go a long way in addressing criticism that human rights concerns are not sufficiently

---

74 Human rights concerns are addressed in Criterion Two of the Common Position. It requires EU Member States "to deny an export license if there is a clear risk that the military technology or equipment to be exported might be used for internal repression." The User's Guide to the Common Position emphasizes that "communications/surveillance equipment can have a strong role in facilitating repression."

75 "European Parliament Resolution of 17 December 2015 on Arms Export: Implementation of Common Position 2008/944/CFSP (2015/2114(INI))," European Parliament, December 17, 2015, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2015-0472+0+DOC+PDF+V0//EN>.

76 See preamble of the draft regulation, recital (6).

77 Green Paper: The Dual-use Export Control System of the European Union: Ensuring Security and Competitiveness in a Changing World," DG Trade, European Commission, 2011, <http://trade.ec.europa.eu/doclib/docs/2011/june/tradoc_148020.pdf>, p. 2.

78 In this regard, the human rights focus also contributes to the expansion of the traditional conception of 'dual-use' towards the 'legitimate versus illegitimate purpose' and 'benevolent versus malevolent use' paradigm that is discussed with regard to cyber surveillance technologies and 'manifest intent.' See for example Johannes Rath, Monique Ischi, and Dana Perkins, "Evolution of Different Dual-Use Concepts in International and National Law and Its Implications on Research Ethics and Governance," *Science and Engineering Ethics* 20:3 (2014), pp. 769–90. This shift in the understanding of 'dual-use' has also become evident in the addition of cyber surveillance technology to the definition of 'dual-use items' in the proposed regulation.

incorporated or easily ignored because of political or economic reasons. The proposal in Article 14 removes the reference to Council Common Position 2008/944/CFSP, which does not explicitly mention threats to, for example, the right to privacy and freedom of expression. Instead, a clear reference to human rights is added and the explanatory memorandum to the new regulation further underlines the risk that the export of cyber-surveillance technology poses to fundamental human rights, including the right to privacy and freedom of expression. To clarify the benchmarks for risk assessments even further, Article 14d could explicitly mention these and other human rights that are particularly exposed to violations through surveillance exports.[79]

EU Member States appear skeptical about the additional emphasis on human rights in the licensing process and are specifically concerned about implementation challenges and the administrative burden for licensing authorities and exporters.[80] Uncertainty could generate a large number of speculative license applications.[81] While some support exists for human rights criteria by, for example, the Netherlands, other Member States seem to perceive the Common Position as a good basis for export licensing assessments and see the problem primarily with its inconsistent application. Business associations have also repeatedly expressed concerns about non-specific human rights standards because they could complicate licensing assessments, increase the need for information collection about their customers, and decrease legal certainty.[82] On the other hand, NGOs and the European Parliament have repeatedly called for stronger human rights criteria.[83]

Given the cautionary remarks by some governments, the Commission proposal retained an overall high level of ambition regarding human rights criteria. To ensure proper implementation, the licensing obligation would need to be accompanied by measures that promote more uniform risk assessment across Member States. The way in which Member States interpret the provision

---

79 "Stellungnahme zum Entwurf der EU-Kommission zur Verordnung Nr . 428 / 2009 über Exportkontrollen von Dual-Use-Gütern," Reporters without Borders, January 2017, <https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Internetfreiheit/20170209_Stellungnahme_ROG_BMWi_Dual_Use_Richtlinie.pdf>.

80 According to Euractiv, a number of Member States have told the Commission that "[t]argeted sanctions are the primary instrument to prevent the misuse of technology for human rights violations." See Catherine Stupp, "Germany Leaves Brussels behind on Surveillance Tech Export Controls," *Euractiv*, 2015, <http://www.euractiv.com/section/digital/news/germany-leaves-brussels-behind-on-surveillance-tech-export-controls/>.

81 "Recording of the INTA Public Hearing on the Reform of the EU Dual-Use Legislation (March 21, 2017)." European Parliament.

82 Instead, these associations emphasize the role of due diligence programs, reporting according to the UN Guiding Principles on Business and Human Rights and the integration of human rights into corporate culture and ethical guidelines. See: DigitalEurope, "DIGITALEUROPE Position Paper on the Review of Export Control Policy in the EU," February 2016, <http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=1125&PortalId=0&TabId=353>; and "EC Dual-Use Review of the EC Dual-Use Regulation," BDI, January 2016, <http://bdi.eu/media/topics/global_issues/downloads/201601_FINAL_BDI-Assessment_Reform_EC_Dual-Use.pdf>.

83 "Human Rights and Technology in Third Countries European," European Parliament, 2015, <http://www.europarl.europa.eu/sides/getDoc.do?type=PV&reference=20150908&secondRef=ITEM-005-08&language=EN>; "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," CAUSE, 2015, p. 17, <https://privacyinternational.org/sites/default/files/CAUSE report v7.pdf>; and Joe McNamee (EDRi), "Consultation on the Export Control Policy Review (Regulation (EC) No 428 / 2009)," 2015, <https://edri.org/files/export_controls_edri.pdf>.

in their export licensing processes is of critical importance for the overall effectiveness of the control regime. While difficult to establish, mandatory risk assessment criteria for licensing procedures could—in comparison to more ambiguous guidelines—significantly increase a consistent and uniform implementation of the new regulation across Member States. In any case, this should also be supplemented by strengthened human rights due diligence procedures and compliance programs that are in some cases already in place—which goes beyond the framework of the dual-use policy review and entails a broader engagement about the use of soft law measures.[84]

Convergence in Interpretation and Use of Catch-all Controls

Similarly, while the dedicated catch-all clause represents an important step towards the control of surveillance exports, there remains a need for clarifications and additional guidance to ensure the catch-all's uniform application. The Commission proposal adds a new type of catch-all to Article 4 of the dual-use regulation, which traditionally allowed Member States to deny the export of non-listed items with potential military or WMD end-use. Article 4d now states that export authorization is required for non-listed items if they are intended "for use by persons complicit in or responsible for directing or committing serious violations of human rights or international humanitarian law in situations of armed conflict or internal repression in the country of final destination." The cyber-surveillance catch-all mechanism would be different in nature from existing ones which deal with a generally more limited range of technologies and destinations and are based on a significant body of knowledge.

Considering the pace of technological development and the variety and ambiguity of cyber-surveillance systems, catch-all provisions provide licensing authorities with the flexibility to respond quickly to critical exports. A catch-all would be useful in future proofing the control system and has so far been less controversial than list-based controls with Member States. Unlike list-based approaches, the application of a catch-all depends entirely on the Member State. Likely results are differences in national implementation and uncertainty among companies, which increase the need for coordination and accountability mechanisms. These problems already occur in the context of the military and WMD catch-all clauses, even though agreed practices and shared standards have been developed.[85] Proponents of the cyber-surveillance technology catch-all have therefore stressed the need to ensure consistent implementation. The European Parliament, for example, highlighted the need "to implement and monitor EU regulations and sanctions relating to ICTs more effectively, including the use of catch-all mechanisms, so as to

---

84 For a detailed assessment of industry self-regulation and the application of CSR guidelines see: Mark Mark Bromley et al., "ICT Surveillance Systems: Trade Policy and the Application of Human Security Concerns," *Strategic Trade Review* 2:2 (Spring 2016), pp. 37–52. The authors argue that self-regulation and CSR can form "a useful complement to export controls in the effort to create improved standards in the export of ICT surveillance systems."

85 Sibylle Bauer and Mark Bromley, "The Dual-Use Export Control Policy Review: Balancing Security, Trade and Academic Freedom in a Changing World," *EU Non-proliferation Paper* 48, SIPRI, March 2016, p. 8. In explaining the need for recasting the dual-use regulation, the Commission pointed out that "divergences in interpretation and application among Member States result in asymmetrical implementation and create competitive distortions within the Single Market.," see: "Report on the EU Export Control Policy Review - Executive Summary of the Impact Assessment (Accompanying the Proposal)" European Commission, 2016.

ensure that […] a level playing field is preserved."[86] Industry is opposed to this measure and states that "catch-all controls should only be a last resort."[87]

The proposal so far does not offer sufficient guidance for Member States to bridge the existing differences in catch-all application and reinforce a policy of no-undercutting. The new regulation envisages a mandatory consultation procedure between licensing authorities to facilitate the use of catch-all provisions and aims at strengthening information exchanges between the Commission and Member States. However, government officials noted concerns regarding a catch-all's uniform implementation in the 2016 Ecorys/SIPRI survey and the March 2017 expert hearing in the European Parliament.[88] Establishing rules for a uniform application would, for example, first require a fundamental understanding regarding the way in which catch-all controls should be employed. Practice differs between governments with regard to the application to an entire destination country or to a specific end-user and whether the provision is used to stop a specific shipment or more broadly as a precautionary or awareness-raising measure.[89] Stakeholders also noted "that if there was a lack of specificity in both the technology and end-users covered by a cyber-surveillance catch-all mechanism it might make it hard to implement" and guarantee uniform implementation.[90] In this regard, it is noteworthy that the language of the catch-all characterizes the recipient as "persons" instead of referring to institutionalized actors such as the armed forces, the police, intelligence, or law enforcement agencies of the state, which would limit the group of relevant end-users.[91] Concerns were also raised with regard to the threshold of "serious violations of human rights" that allows recourse to the catch-all.[92] A greater role of the Commission in coordinating implementation and issuing guidance, which is sometimes suggested, would likely raise concerns with some Member States.[93]

---

86 Frans Timmermans, "Human Rights and Technology in Third Countries European," Speech to the European Parliament, September 7, 2015, <https://ec.europa.eu/digital-single-market/en/news/human-rights-and-technology-third-countries>.

87 "EC Dual-Use Review of the EC Dual-Use Regulation," BDI, January 2016, <http://english.bdi.eu/media/topics/global_issues/downloads/FINAL_BDI-Assessment_Reform_EC_Dual-Use.pdf> and "DIGITAL EUROPE Position Paper on the Review of Export Control Policy in the EU," DigitalEurope, October 2014, <http://www.europarl.europa.eu/meetdocs/2014_2019/documents/droi/dv/412_digitaleurope_position_paper_/412_digitaleurope_position_paper_en.pdf>.

88 An expert of the German Federal Office for Economic Affairs and Export Control noted that consultations between EU Member States based on Art. 4 of the proposal might not lead to an understanding on common standards. See: "Recording of the INTA Public Hearing on the Reform of the EU Dual-Use Legislation (March 21, 2017)," European Parliament, 2017

89 Sibylle Bauer and Mark Bromley, "The Dual-Use Export Control Policy Review: Balancing Security, Trade and Academic Freedom in a Changing World," *EU Non-proliferation Paper* 48, SIPRI (March 2016), p. 6; and Ecorys and SIPRI, "Final Report: Data and Information Collection for EU Dual-Use Export Control Policy Review," (2015), p. 103.

90 Ibid, 219–20.

91 In comparison, Article 6 of the Common Position 2008/944/CFSP states that the criteria only apply to dual-use goods and technology "if the end-user will be armed forces or internal security forces." However, many cyber surveillance technologies, such as LI equipment, are operated at the level of (privately run) network operators.

92 "Recording of the INTA Public Hearing on the Reform of the EU Dual-Use Legislation (March 21, 2017)," European Parliament.

93 Marietje Schaake, "Written Submission to the Public Online Consultation on the Export Control Policy Review (Regulation (EC) No 428/2009)," 2015, <http://trade.ec.europa.eu/doclib/docs/2015/november/tradoc_154004.pdf>.

In comparison to measures aimed at the convergence of the new catch-all, other provisions aimed at "leveling the playing field" in export licensing procedures are relatively uncontroversial and were welcomed by a broad range of actors. These include the development of a common IT infrastructure as a shared platform to support an enhanced exchange of information between export control authorities, an EU-wide capacity-building program and outreach efforts towards non-EU countries to disseminate best practices.[94,95,96] Licensing authorities also emphasized the weaknesses of the existing system, in which information sharing is mostly limited to authorization denials.[97] Access to information in other areas, such as granted licenses, critical destinations and end-users, incidents, and violations could help to improve national risk assessment procedures and harmonize outcomes. Sharing this export data has traditionally been difficult because of national and commercial interests but will be crucial to avoid disparate national policies that facilitate licensing avoidance and create loopholes in enforcement mechanisms for cyber-surveillance technologies.[98]

Overall, the Commission proposal represents a considerable improvement to the existing export control framework for cyber-surveillance technologies. In light of the cautionary remarks by Member State governments and industry groups, the Commission presented a surprisingly comprehensive and ambitious proposal. The changes to Regulation 428/2009 will now need to be agreed upon by the Member States and the European Parliament. One further issue to consider in this process is the need for greater transparency on export licensing decisions and outreach to affected entities, experts and civil society. Over the last years, many actors have pointed out that more reliable information and data on exports is needed to ensure that existing and future control measures are clear, effective, and consistent. The proposal falls short of calling on governments to publish comprehensive data concerning export license applications for surveillance technologies. Greater openness would encourage independent systematic research and contribute to accurate impact assessments, legal clarity, and better public understanding of the issue.

Conclusion: Chasing a Moving Target

It will always prove difficult to ensure that legislative processes keep up with technological developments, especially when it regards the internet. Advances in cyber-surveillance capabilities

---

94 The European Commission proposed an extension of information sharing through a catch-all database recording catch-all licensing requirements, end-users and items of concern.

95 A critical aspect is to address the lack of expertise and staff at both Member State and EU level, which undermines the effectiveness of existing controls on cyber surveillance technologies. The Commission has suggested setting up "technical expert groups" (Article 21) which bring together key industry and government experts into a dialogue on the technical parameters for controls. Creating a pool of experts to assist licensing authorities in the area of cyber surveillance technologies could be a meaningful first step in this direction. Capacity building can also promote a uniform approach and is used to contribute to international convergence of export controls beyond the EU.

96 Green Paper: The Dual-use Export Control System of the European Union: Ensuring Security and Competitiveness in a Changing World," DG Trade, European Commission, 2011, <http://trade.ec.europa.eu/doclib/docs/2011/june/tradoc_148020.pdf>, p. 2.

97 Interview with the author, Expert in the Federal Ministry of Economic Affairs and Energy.

98 Sibylle Bauer and Mark Bromley, "The Dual-Use Export Control Policy Review: Balancing Security, Trade and Academic Freedom in a Changing World," *EU Non-proliferation Paper* 48, SIPRI, March 2016.

have so far outstripped the ability of institutions of governance to modernize the control framework. The unregulated export of cyber-surveillance technologies has exposed individuals to new risks to their human rights and created security concerns. Laws and regulation currently chase a moving target.

On the European level, the outcome of the export policy review represents an ambitious response to the control challenge, magnifying the effect of existing control lists and licensing procedures and aiming at supplementing the existing framework with requirements specifically designed to oversee the export of cyber-surveillance technology. However, considering the actions of individual Member States that introduced additional controls on a national level, the Commission proposal should also be seen as a step towards leveling the European playing field. It is likely that the draft regulation will face some resistance by Member State governments and therefore might be subject to changes. Going forward, it will be up to the European Parliament, which has repeatedly shown its determination to improve the control regime on cyber-surveillance technology, to make sure that progress is not stymied and innovative steps not diluted.[99]

Further action at the EU and WA level does not guarantee that other key technology suppliers will introduce similar controls but certainly has the potential to limit the spread of some of the most contentious technologies and set an example for others. Arguments about the replaceability of European cyber-surveillance exports, potential circumvention or relocation opportunities, and distortions of competition should not preclude governments from enacting stricter controls on the EU or even national level. On the other hand, it remains true that an effective control regime should include as many countries as possible. Even with a new control system on the European level, a clear need will remain to coordinate with countries within the WA and beyond and especially key supplier countries should be approached with ideas to establish a broader regime. This could, for example, include Israel, which has a significant dual-use industry and made considerable progress in implementing export controls on cyber-surveillance technology.[100] In light of Brexit, it will also be crucial to ask whether UK export controls will remain compatible with EU controls and to institutionalize coordination arrangements.[101]

Working towards a broader regime would enjoy support by civil society and industry associations alike because it would address concerns about an uneven global playing field.[102] However, similar undertakings such as the multilateral Arms Trade Treaty show clear limitations of such attempts. Despite the agreement's focus on conventional weapons, products with a clear impact

---

99 Frans Timmermans, "Human Rights and Technology in Third Countries European," Speech to the European Parliament, September 7, 2015, <https://ec.europa.eu/digital-single-market/en/news/human-rights-and-technology-third-countries>; "Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries," European Parliament, 2014/2232(INI), August 2015, <http://www.europarl.europa.eu/oeil/popups/summary.do?id=1401513&t=e&l=en>.

100 Doron Hindin, "Can Export Controls Tame Cyber Technology?: An Israeli Approach," *Lawfare Blog*, February 12, 2016, <https://www.lawfareblog.com/can-export-controls-tame-cyber-technology-israeli-approach>.

101 Mark Bromley, "Brexit and Export Controls: Entering Uncharted Waters," SIPRI, 2016, <https://www.sipri.org/commentary/topical-backgrounder/2016/brexit-and-export-controls-entering-uncharted-waters>.

102 "A Critical Opportunity: Bringing Surveillance Technologies within the EU Dual-Use Regulation," CAUSE, 2015, <https://privacyinternational.org/sites/default/files/CAUSE report v7.pdf>; and "DIGITALEUROPE Position Paper on the Review of Export Control Policy in the EU," DigitalEurope.

on security, stability, and human rights, negotiations were difficult and a significant number of states have not yet ratified the agreement. Regarding dual-use cyber-surveillance technologies, which are more ambiguous in terms of definitions and risks attached, international controls will be even more difficult.

Overall, policy-makers must be aware that trade restrictions on cyber-surveillance technology are not a panacea. Yet, subjecting these heterogeneous products and services to an export licensing regime can curb their unregulated spread and promote broader norms. Even when they are not invoked to restrict a transfer, export controls can act as an essential accountability and transparency mechanism, thus shedding light on this secretive trade and informing future regulatory responses. To be truly effective, export controls will need to be complemented by foreign policy initiatives that raise awareness of the problem, build a broader regime with common standards, and promote and protect human rights online and offline.

Is There a Common Understanding of Dual-Use?: The Case of Cryptography

VERONICA VELLA[1]

Abstract

This article explores the dual-use concept by focusing on the specific case of export controls on cryptographic products. The analysis demonstrates different implementation models and interpretations adopted by states. Although adhering to the same multilateral export control regimes, states employ different approaches when it comes to implementation. The United States and the European Union approach to cryptography are used as case studies to confirm this hypothesis. This paper acknowledges the necessity of revisiting the dual-use concept over time as technology and understanding develop.

Keywords

Dual-use, cryptography, export controls, Weapons of Mass Destruction (WMDs), Wassenaar Arrangement, intangible technology transfer

The Concept of Dual-Use in Practice

An analysis of politically and legally binding documents governing dual-use trade shows the lack of an internationally legally binding definition of dual-use. Existing instruments define the term in different ways, such as being linked to military capabilities, nuclear proliferation, covering the full spectrum of Weapons of Mass Destruction (WMD), or even encompassing the human security approach to dual-use put forward by the European Parliament.[2]

If a common understanding of dual-use in politically and legally binding documents does not exist, then what do these instruments have in common? One answer may be that the lack of an

1 Veronica Vella graduated in Global Politics, European Union, and Euro-Mediterranean Relations at the University of Catania (UC) and the University of Liège (ULg) - Double Master Degree Program. She has worked at the University of Liege in the European Studies Unit (ESU ULg).

2 See Annex I of this article for a full comparative analysis of existing definitions.

internationally legally binding definition has been mitigated or even replaced by lists of dual-use items that have resulted from bargaining and compromise over time. Consequently, lists, in addition to being the commonality of the different instruments employed to control dual-use commerce, have become the dual-use concept itself. In theory, since control lists are similar for all export control regime members, their understanding should be the same as well, and implementation should be uniform and smooth. However, the biggest distinction in the understanding of the dual-use concept lies in the different export control systems employed by states.

The following sections use the case study of cryptography to demonstrate whether a common understanding of dual-use exists from an empirical perspective. The case study aims to verify the conformity of lists governing dual-use trade and attest to a common understanding of dual-use at the implementation level.

Cryptography as a Dual-Use Technology

Cryptography is one of the most complex areas of the security industry. Increasingly, the issue of export controls on cryptographic products has been raised.[3] Several factors, such as the growing international trade of information technology and services, companies' increased interest in high-technology areas, and the centralized storage of personal and sensitive data and its transfer across digital networks have created a greater necessity for information security, whose key component is cryptography.[4]

> *Cryptography is defined as "the discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification or prevent its unauthorized use. Cryptography is limited to the transformation of information using one or more 'secret parameters' (e.g., crypto variables) or associated key management."*[5]

Products that are designed or modified to use cryptography employing digital techniques performing a cryptographic function are ruled by encryption export controls. Most countries, to varying degrees, regulate encryption as a dual-use item, having both civilian and military applications.

The United States was the first country to pioneer efforts to regulate encryption during the Cold War.[6] With the aim of harmonizing regulations on the export and import of dual-use

---

3 Some examples include the case of J. Daniel Bernstein challenging the constitutional validity of the US export system; the struggle against encryption limitations held by international privacy advocates in political debates (such as the Electronic Privacy Information Centre the Electronic Frontier Foundation, Privacy International, Cyber Rights & Cyber Liberties-UK, and the Global Internet Liberty Campaign); the DigitalEurope position on the EU-US Regulatory Cooperation; the issues raised by E. Snowden a couple of years ago; and more recently it has been questioned and reported in the press the possible role that cryptography has had in the Paris terrorist attacks (as if restricting encryption would not have prevented the them).

4 Nathan Saper, "International Cryptography Regulation and the Global Information Economy," *North Western Journal of Technology and Intellectual Property* 11:7 (2013), p. 673.

5 The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies, "List of Dual-use Goods and Technologies and Munitions list," WA-LIST (16) 1, December 8, 2016, p. 209.

6 Nathan Saper, "International Cryptography Regulation and the Global Information Economy," *North Western Journal of Technology and Intellectual Property* 11:7 (2013), p. 677.

technologies, many countries have agreed to a set of principles, for example the Wassenaar Arrangement (WA).[7] However, although the WA sets general parameters for import and export control to which its Member States largely adhere, they are not binding and are implemented at the discretion of each country. Thus, until Member States implement these provisions in national legislation, the controls have little effect.

Cryptography is fully regulated by one of the four main export control regimes and partially regulated in two others. The Australia Group (AG) Common Control Lists do not control cryptography, whereas the Missile Technology Control Regime (MTCR) Equipment, Software and Technology Annex refers to "decryption" in Category II Item 11,

> *"Receiving Equipment for Global Navigation Satellite Systems" as "having any of the following characteristics, and specially designed components therefor: [...] 1. Designed or modified for airborne applications and having any of the following: [...] 2. Employing decryption, designed or modified for military or governmental services, to gain access to GNSS secure signal/data [...]."*

The Nuclear Suppliers Group's (NSG) list of Nuclear-related Dual-Use Equipment, Materials, Software, and Related Technology denotes cryptography in Part II under the heading "Uranium isotope separation equipment and components (Other Than Trigger List Items) - 3D Software." It specifies cryptography as "software or encryption keys/ codes specially designed to enhance or release the performance characteristics of equipment." Further, the heading "Test and measurement equipment for the development of nuclear explosive devices, Software 5.D.1" mentions "Software or encryption keys/codes specially designed to enhance or release the performance characteristics of equipment not controlled in Item 5.B.3. so that it meets or exceeds the characteristics specified in Item 5.B.3."

Finally, the Wassenaar Arrangement controls cryptographic products as dual-use items under Category V, Part II of the "Information Security" section of its List of Dual-use Goods and Technologies and Munition List. The Cryptographic Information Security section states, "Information security systems, equipment and components, as follows: [...] Designed or modified to use cryptography for data confidentiality having in excess of 56 bits of symmetric key length, or equivalent… where that cryptographic capability is usable without cryptographic activation or has been activated." However, some exceptions have been established in the Cryptography Note and in the Note to the Cryptography Note.[8]

---

7 The Wassenaar Arrangement (WA) succeeded the Co-ordinating Committee on Multilateral Export Controls (COCOM), which existed during the Cold War-era. It was established in 1994 in order to contribute to regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations.

8 Note to the Cryptography Note: 1. To meet paragraph a of Note 3, all of the following must apply: (a) The item is of potential interest to a wide range of individuals and businesses; and (b) The price and information about the main functionality of the item are available before purchase without the need to consult the vendor or supplier. A simple price enquiry is not considered to be a consultation. 2. In determining eligibility of paragraph a. of Note 3, national authorities may take into account relevant factors such as quantity, price, required technical skill, existing sales channels, typical customers, typical use or any exclusionary practices of the supplier. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies, "List of Dual-use Goods and Technologies and Munitions list," WA-LIST (16) 1, December 8, 2016, p. 87.

Different Approaches to Controlling Cryptography: The United States vs. The European Union

This section considers the EU and US implementation approach towards controlling cryptography. This comparison is a useful starting point for any investigation into the global framework for encryption regulation since the two countries have the most developed and documented laws regarding encryption.

United States

The United States is one of the global leaders in encryption technology and therefore has significant influence on international trade and policies on encryption. Accordingly, debates on encryption in the US have an impact far beyond national borders.

US trade of dual-use items is regulated by the Department of Commerce Bureau of Industry and Security (BIS) which implements its authority through the Export Administration Regulations (EAR).[9] The EAR defines dual-use as items as those "[having] civil applications as well as terrorism and military or weapons of mass destruction (WMD)-related applications."[10] This definition seems to reflect a wider US understanding of dual-use that extends beyond the traditional dichotomy of civilian versus military, including a terrorist dimension.

As noted in 15 CFR 738, the Commerce Control List (CCL) of export controlled items covers ten categories ranging from nuclear materials to space vehicles. Within each category both export controlled physical objects and export controlled digital objects (software and "technology," i.e., information) are controlled. Encryption is covered under Category V, "Telecommunications and Information Security." It is important to note that this particular entry, listed in the CCL under a particular Export Control Classification Number (ECCN), may be controlled for multiple reasons: encryption software and technology are marked as being controlled not only under the special "EI" Reason for Control but also under the more general "NS" (national security) and "AT" (anti-terrorism) Reasons for Control.[11,12]

Although the US is a WA member, it does not apply the General Software Note to "software" controlled by Category V – part II "Information Security" and generally maintains stricter controls than what is required by the arrangement.[13,14,15] The US employs the same definition of cryptography as the WA yet takes a broad view of the scope of the encryption controls given

---

9 The EAR is part of the US Code of Federal Regulations (CFR); more specifically, they are in Title 15 of the CFR, "Commerce and Foreign Trade," Chapter VII, "Bureau of Export Administration, Department of Commerce (Parts 700-799)," Subchapter C, "Export Administration Regulations;" hence the EAR are also sometimes referred to as 15 CFR chapter VII subchapter C or 15 CFR Parts, pp. 730-774.

10 US Department of Commerce, "EAR – Part 730," BIS, January 4, 2017, p. 2.

11 There is an "EI" Reason for Control applied just to encryption items.

12 US Department Of Commerce, "EAR – Part 738," BIS, November 25, 2016.

13 *General Software Note* serves not to control "software" which is (1) generally available to the public, according certain criteria, (2) "in the public domain," (3) the minimum necessary "object code" for the installation, operation, maintenance (checking) or repair of those items whose export has been authorized.

14 US Department Of Commerce, "EAR – Part 774, The Commerce Control List," BIS, September 20, 2016, p. 1.

15 Bert-Jaap Koops, "Crypto Law Survey, Overview per Country," February 2013, <www.cryptolaw.org>.

that it includes controls on products that make calls to the encryption functionality of a third party product, activation codes to activate "dormant" encryption functionality.[16,17]

The US has been one of the most vocal advocates of restrictions on the right to use and export encryption, mainly driven by its prerogative to safeguard national security and foreign intelligence gathering capabilities, and increasingly by terrorist concerns. Initially, cryptographic products were controlled under the International Traffic in Arms Regulations (ITAR).[18] Considering the "commodity jurisdiction" procedure provided by the ITAR, a specific item was considered controlled depending on whether it came under the US Munitions List. If so, the item required a license before it could be exported. Munitions licenses were granted by the Department of State on a case by case basis. It was not until J. Daniel Bernstein challenged the constitutional validity of this licensing system that cryptographic export was transferred to the EAR, which essentially replicates the impugned ITAR controls on cryptographic technologies.[19,20]

The liberalization of US export policies started in 1998, when the Clinton administration announced a new policy to reform the strict export regime. However, during the reform process, the US also proposed domestic controls on the use of encryption which would enable law enforcement officials to legally access encryption keys when necessary.[21]

The US has been a strong advocate of so-called "key escrow and key recovery systems" which involve third party access to private keys or the ability to access data in plain text. Such systems authorize a third party, such as government agency, or a Trusted Third Party, usually connected with the government, to store cryptographic keys and provide them to a government agency when requested.[22] The US strongly pressured the international community to adopt this system. However, doing so provoked a strong reaction from international privacy advocates, security experts and civil liberties groups.[23] The opponents of this system maintained that it would

---

16 The discipline that embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification or prevent its unauthorized use. "Cryptography" is limited to the transformation of information using one or more "secret parameters" (e.g., crypto variables) and/or associated key management. EAR- Part 772, p. 13. WA-LIST (16) 1, December 8, 2016, p. 209.

17 Jasper Helder, and John F. McKenzie, "Encryption Export Controls: A Comparative Analysis between the EU and the US," Annual International Trade Compliance Conference, Netherlands: November 8, 2013, p. 4, <http://www.hhp.co.id/files/Uploads/Documents/International%20Trade%20&%20Compliance%20Event/Jasper%20Helder%20and%20John%20McKenzie_Encryption%20Export%20Controls_A%20Comparative%20Analysis%20between%20the%20EU%20and%20the%20U.S..pdf>.

18 The ITAR regulates exports of items and services specifically designed for military applications while the EAR regulate exports of commercial items with potential military applications ("dual-use" items).

19 The licensing scheme under ITAR violated his First Amendment right to free speech.

20 See for example Sarah Andrews, "Who Holds the Key? – A Comparative Study of US and European Encryption Policies," *The Journal of Information, Law and Technology (JILT) (*February 2000*),* p. 8-9.

21 The first attempt to restrict domestic use came in 1993 when the government developed the Escrowed Encryption Standard Initiative aimed at providing citizens with a good level of security for communications while at the same time preventing transmission of data in total secrecy.

22 D. Maniotis, M.T. Marinos, A. Anthimos, I. Iglezakis, and G. Nouskalis, *Cyber Law in Greece* (Netherlands: Kluwer Law International, 2011), p. 69.

23 For example, the Electronic Privacy Information Centre the Electronic Frontier Foundation, Privacy International, Cyber Rights & Cyber Liberties (UK), and the Global Internet Liberty Campaign.

present a violation of the right to privacy, besides the fact that such systems are ineffective against criminals who merely use other encryption methods to avoid detection.[24] Moreover, it is important to mention that in the US there is no specific law protecting the right to privacy of personal information. This area is ruled by a piecemeal collection of constitutional and statutory laws and self-imposed industry regulations.[25]

US export controls have been subject to a new wave of liberalization triggered by changes to the EU export regulations.[26] As a consequence, a license exception was introduced for the export of any crypto product to *any* end-user in the EU. Export restrictions to terrorism supporting countries were maintained. In January 2011, a minor amendment was made to the EAR. Publicly available mass-market encryption object code software, and publicly available encryption object code of which the corresponding source code falls under License Exception TSU, are no longer subject to the EAR.[27]

When exporting cryptographic products under the EAR, there are two important factors exporters must consider. First, the attributes of the software to be exported due to concern over key length. Indeed, Category V Part II of the EAR specifies that encryption systems with key lengths of 56 bits or less for symmetric systems, or 512 bits or less for asymmetric systems, can be exported without restriction. Strong encryption systems, which use longer keys, face export restrictions.[28] Moreover, there is an exemption for "mass market" encryption products, according to which if an encryption product is generally available to the public, for home or personal use, without continuing support by the supplier (e.g., a personal email security program), then its export is not restricted. A final important exemption is for products "when accompanying their user for the user's personal use or as tools of the trade […];" this allows users to, for example, travel with laptops and mobile phones that contain encryption capabilities.[29]

In addition, exporters must consider to whom the software is being sold, thus including the specific attributes of the customer's location, which can be problematic. Indeed, the exporter must indicate and ensure that their customers are neither located in an embargoed country nor are "Specially Designated Nationals."[30] However, contrary to other countries' export control regimes, the EAR makes no distinction between the physical shipment of tangible items from the US to a foreign country and the electronic transmission of software or technology from

---

24 Sarah Andrews, "Who Holds the Key? – A Comparative Study of US and European Encryption Policies," *The Journal of Information, Law and Technology (JILT) (*February 2000*),* p. 4.

25 Ibid, 14.

26 Bert-Jaap Koops, "Crypto Law Survey, Overview per Country," February 2013, <www.cryptolaw.org>.

27 Ibid.

28 U.S. Department Of Commerce, "EAR – Category 5 Part 2, "Information Security," BIS, September 20, 2016.

29 Nathan Saper, "International Cryptography Regulation and the Global Information Economy,*" North Western Journal of Technology and Intellectual Property* 11:7 (2013), p. 680-681.

30 The Office of Foreign Assets Control (OFAC), an agency within the US Treasury Department, administers sanctions programs against specific countries, restricting the export of sensitive products and materials—including cryptography software—to those locations. In addition, OFAC administers restrictions against exports to specially designated individuals and entities, known as "Specially Designated Nationals" ("SDNs"); exports to those individuals and entities are generally prohibited.

the US to a person or entity located abroad.[31] For export control purposes, any such physical shipment or electronic transmission is an export that must be performed in accordance with the requirements and restrictions embodied in the EAR. Thus, section 734.2(b)(1) of the EAR defines the term export to include any "actual shipment or transmission of items subject to the EAR out of the United States." All this proves to be problematic when firms that sell encryption software over the internet must adopt measures to screen their customers to assure their location, and it is yet unclear what kinds of steps such firms can take to ensure compliance.[32]

Although its export control system is based on its commitments under multilateral export control regimes, "the US also maintains unilateral controls on a wide range of dual-use items predominantly for anti-terrorism reasons."[33] The US maintains certain "anti-terrorism export controls" on those encryption products that are excluded from controls. Specifically, encryption products that are subject to export controls are generally classified under 5A002 (hardware) and 5D002 (software). Export licenses or other authorizations (such as export license exceptions) are required in order to export those 5A002 and 5D002 encryption products from the US. However, there are certain products with encryption functions and features that are excluded from the controlled categories.[34] Those excluded products are subject to certain "anti-terrorism" export controls. In the encryption provisions of the US CCL, encryption products that are excluded from 5A002 (hardware) and 5D002 (software) are classified for US export control purposes under 5A992 (hardware) and 5D992 (software).[35] Those entries on the CCL indicate that products classified under those 5A992 and 5D992 categories are controlled for "AT" (or anti-terrorism) purposes.[36] Therefore, under both the US Commerce Country Chart and the anti-terrorism provisions of Part 742 of the EAR, the products that are subject to those AT export controls are restricted for export to those countries that have been designated by the United States Government as terrorism supporting countries.[37]

European Union

Article II.I of European Council Regulation (EC) 428/2009, otherwise known as the EU Dual-Use Regulation, defines dual-use as "items, including software and technology, which can be used for both civil and military purposes, and shall include all goods which can be used for both

---

31 John F., McKenzie, "United States Export Controls on Internet Software Transactions," Baker & McKenzie, August 2010, p. 3.

32 Nathan Saper, "International Cryptography Regulation and the Global Information Economy," *North Western Journal of Technology and Intellectual Property* 11:7 (2013), p. 681.

33 Office of the Coordinator for Counter-terrorism, The Global Challenge of Chemical, Biological, Radiological, and Nuclear (CBRN) Terrorism, 2011, <https://www.state.gov/j/ct/rls/crt/2013/224827.htm>.

34 Examples of those excluded products include (i) products that use a very weak encryption algorithm only (e.g., a symmetric encryption algorithm with a key length of 56 bits or less); (ii) products that qualify as "mass market" encryption items; and (iii) products that use encryption exclusively for authentication, password protection or other forms of access control to digital resources, but do not provide any data encryption functionality

35 US Department of Commerce, "EAR – Category 5 Part 2 - Information Security," BIS, September 20, 2016.

36 US Department of Commerce, "EAR – Part 742, Control Policy - CCL Based Controls," BIS, January 2017.

37 US Department of Commerce, "EAR - Supplement No. 1 to Part 738 – Commerce Country Chart," BIS, November 4, 2016; US Department of Commerce, "EAR – Part 742, Control Policy - CCL Based Controls," BIS, January 15, 2017.

non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices."[38] This definition cumulates "purposive" understanding of this term because it first refers to military and non-military purposes (WA, AG, MTCR definitions), and then refers to nuclear and non-nuclear purposes (NSG definition), including nuclear terrorism.[39]

However, especially after the Arab Spring began in 2010, and considering the deep instability of the African continent and the Middle East, the concern of dual-use trade has expanded in the EU towards a concern for human rights in the export control context. By way of illustration, the European Parliament (EP) proposed a legislative resolution in 2012 to extend the scope of dual-use.[40] Debates on this particular issue, mainly linked to dual-use technologies, are still ongoing as part of the review of the Regulation. Members of the EP as well as members of the Commission call for "taking into consideration human rights as a new dimension of export controls," suggesting establishing human rights as a reason for control and possibly denial of export.[41] These debates arose after the discovery that during the uprisings in Tunisia and Egypt, information and communication technologies provided by European companies played a role in aiding and assisting the government's violation of the freedom of expression, freedom of press and access to information.[42]

The recent European Commission proposal to amend Council Regulation No. 428/2009 has introduced the issue of preventing human rights violation associated with certain cyber-surveillance technology.[43] The proposal adds to the definition of dual-use, in Article II, a paragraph as follows,

> *"Cyber-surveillance technology which can be used for the commission of serious violations of human rights or international humanitarian law, or can pose a threat to international security or the essential security interests of the Union and its Member States."*[44]

As far as cryptography is concerned, generally, EU Member States are unified in their commitment to a liberal framework for encryption regulations, even though there has not yet been formal

---

38 Council Regulation (EC) No. 428/2009 of 5 May 2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items, Official Journal of the European Union (L 134/1) of May 29, 2009.

39 Quentin Michel, Sylvian Paile, Maryna Tsukanova and Andrea Viski, *Controlling the Trade of Dual-Use Goods - A Handbook*, (Brussels, Peter Lang, 2013) p. 81.

40 "Export Controls of Dual-use Items," CRE 24/11/2014 - 18, European Parliament, February 18, 2015, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20141124+ITEM-018+DOC+XML+V0//EN>.

41 Ibid.

42 "Inquiry into Role of European Companies in Violation of Human Rights," European Parliament, March 9, 2011, <http://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=E-2011-002212&language=SL>.

43 EU Commission, "Proposal for a Regulation of the European Parliament and of the Council Setting Up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (recast)," COM (2016) 616 final, Brussels, 2016, <http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154976.pdf>.

44 Ibid.

harmonization of encryption policies among them.[45] The export control laws of Member States regarding encryption products are uniformly regulated under European law, although each state may have additional regulations concerning the import, supply, use or export of encryption items.

At present, the governing legislation is the Commission Delegated Regulation (EU) 2015/2420 of October 2015 amending Council Regulation (EC) No. 428/200.[46] Before this amendment, the Commission Delegated Regulation (EU) No. 1382/2014 of October 2014 replaced and updated the EU control list to reflect decisions take in export control regimes in 2011, 2012 and 2013.[47] The update incorporated some 400 changes, including the addition of new controls, the removal of some controls, changes to certain technical parameters and other amendments.[48] Among the most significant changes is the inclusion of an additional "note to cryptography note" in order to be in line with the WA and other international agreements.[49]

In addition, the EU has adopted a General Technology Note and a General Software Note that excludes information and software within the public domain from the Control List. Cryptography and information security products are included in Annex I of the control list and are subject to a licensing regime as regard exports from the European Union.

Similarly to the US, the EU takes a broad view of the scope of encryption controls. Indeed, it also includes activation codes to activate "dormant" encryption functionality, but unlike the US, it has always controlled components for "mass market" encryption items.[50] However, encryption products specially designed or modified for military use are subject to export control under national regulations of EU Member States with respect to military items.

The most significant difference between EU and US encryption export controls lies in their respective clarity in defining what is and what is not controlled. Indeed, generally EU controls are very clear whether an item is to be controlled or not and there is no equivalent to US anti-terrorism controls on an EU level even if some Member States can introduce national controls beyond the EU Regulation.[51,52] Nonetheless, if the US employs the "exceptionalism" of anti-terrorism, the EU applies the "exceptionalism" of human rights. In this regard, Article VIII of the EU Regulation clarifies that "a Member State may prohibit or impose an authorization

---

45 Sarah Andrews, "Who Holds the Key? – A Comparative Study of US and European Encryption Policies," *The Journal of Information, Law and Technology (JILT),* February 2000, p. 13.

46 European Commission Delegated Regulation No. 2420/2015 amending Council Regulation (EC) No. 428/2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items, Official Journal of the European Union, October 12, 2015.

47 Commission Delegated Regulation (EU) No. 1382/2014 of 22 October 2014 Amending Council Regulation (EC) No. 428/2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items, Official Journal of the European Union (L 371/1), December 30, 2014.

48 Ibid.

49 Ibid.

50 Jasper Helder and John F. McKenzie, "Encryption Export Controls: a Comparative Analysis between the EU and the US," Annual International Trade Compliance Conference, Netherlands: November 8, 2013, p. 18.

51 There is no equivalent to US anti-terrorism controls such as 5A992, 5D992, 5E992.

52 Jasper Helder and John F. McKenzie, "Encryption Export Controls: a Comparative Analysis between the EU and the US," Annual International Trade Compliance Conference, Netherlands: November 8, 2013, p. 22.

requirement on the export of dual-use items not listed in Annex I for reasons of public security or *human rights consideration*."[53]

Indeed, as far as cryptography is concerned, many EU licensing authorities consider encryption for governmental use to be a potential human rights issue. A few examples of encryption related human rights impact are, for example: (1) German unilateral controls for certain hardware and software for Terrestrial Trunked Radio (TTR) for Sudan, (2) increased scrutiny by Dutch authorities of encryption exports to Lebanon, (3) the exception for the supply of certain encryption items to Iran under EU sanctions, (4) Netherlands brokering controls requiring individual pre-notification of brokering for the supply of controlled items for "sensitive countries," and (5) UK license refusals for encryption communications equipment.[54,55]

The UK presents an exception to the overall EU approach towards this issue. Indeed, the UK has specific requirements relating to the export of certain cryptographic items when exported from the UK under a EU General Export Authorization (GEA). These requirements consist in providing "details of information, which is in a person's possession, or other information as that person can be reasonable be expected to obtain."[56] Such information should be submitted to the UK Export Control Organization (ECO) via email within 30 days of first export.

Overall, despite the EU common framework, Member States implement encryption controls differently and still have dissimilar national laws in some cases.[57] The EU approach towards cryptography reflects its understanding of dual-use as also related to human rights violations in this regard. Moreover, the EU does not have equivalent to US anti-terrorism controls such as 5A992, 5D992, 5E992. Indeed, "anti-terrorism export controls" has proved to be a unique feature of US implementation.

What about 'International Competitiveness'?

As shown above, the EU and US approach towards cryptography, and more generally to the dual-use concept, is not the same, nor does it seems to be coherent. These different understandings may damage *inter alia* international competitiveness. In this regard, and as a further demonstration of the inconsistency of these two approaches, it is useful to mention the point of view of an important stakeholder, namely DigitalEurope, a European organization that represents the digital technology industry and seeks to ensure industry participation in the development and implementation of EU policies.[58] In the framework of the much-discussed *Transatlantic Trade*

---

53 Council Regulation (EC) No. 428/2009 of 5 May 2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items, Official Journal of the European Union (L 134/1) of May 29, 2009.

54 Afghanistan, Angola, Belarus, Burma, Congo, Egypt, Eritrea, Guinea, India, Iraq, Iran, Israel Ivory Coast, Lebanon, Liberia, Libya, North-Korea, Pakistan, Sudan, Syria, Zimbabwe, South Sudan.

55 Jasper Helder and John F. McKenzie, "Encryption Export Controls: a Comparative Analysis between the EU and the US," Annual International Trade Compliance Conference, Netherlands: November 8, 2013, p. 24.

56 "Additional UK Requirements for Cryptography Items Exported under an EU GEA," EU General Export Authorizations, <https://www.gov.uk/european-union-general-export-authorisations>.

57 *See* Figure 2 in Annex II.

58 "About Us," DigitalEurope, <http://www.digitaleurope.org/Aboutus.aspx>.

and Investment Partnership (TTIP) between the EU and the US, DigitalEurope addresses a paper containing its comments and suggestions about it.

The organization underlines the divergent policy approaches adopted by the EU and the US towards the ICT industry. The two systems demonstrate differences in their regulatory systems and in their approaches to risk management, making the achievement of a certain level of harmonization difficult. Even when principal regulatory objectives are equivalent, in practice product requirements imposed by the EU and US technical regulations in certain cases diverge.[59] Indeed, given that the ICT industry generally operates on a global scale, dissimilarities in standard requirements involve the implementation of more than one standard for the same functionality, and hence lead to duplicated implementation efforts and costs. DigitalEurope members offer products, such as hardware or software with cryptographic capabilities, classified as dual-use items. It argues that EU and US export control regulations require that every export of dual-use item shall be performed according these regulations, which envisage either an export authorization/license or a license exception. Nevertheless, because the implementation of export controls is a national responsibility, the administrative procedures for compliance and the method for controlling dual-use items differ between the controlling countries.[60] Hence a problem arises of damaged international competitiveness.

The latter may be further proved by glancing at other countries' approaches to cryptography. Figure II in Annex II provides a general view of international engagements towards import and export controls, and domestic law and regulations on crypto use.[61] If on the one hand nothing new emerges from this figure (since the weaknesses of dual-use export controls—i.e., the lack of uniformity in implementation and even acceptance of these systems by states—are well known), on the other hand it suggests that a strong dual-use export control system is needed worldwide in order to be effective and assure competitiveness and security.

China is one of the most challenging environments for cryptography use and regulations.[62] Both import and export of cryptographic products are highly regulated, and, specifically, encryption is regulated by the National Commission on Encryption Code Regulations (NCECR).[63] Encryption products cannot be sold or imported in China without prior approval by NCECR, and individuals and firms can only use cryptographic products approved by NCECR. This restriction also applies to foreign individuals and firms operating in China as they must receive approval to use their encryption systems. China is not a member of the WA, which means WA Member States are not allowed to export chip technology to China.

Unlike in the US and the EU, all encryption products in China, regardless of key strength or other factors, are fully regulated.[64] Nevertheless, importing encryption products and equipment

---

59 "Digitaleurope Position on the EU-US Regulatory Cooperation," Digital Europe, November 5, 2013, Brussels, p. 1.

60 Ibid, 15.

61 However, it is important to note that it is updated to 2013.

62 Nathan Saper, "International Cryptography Regulation and the Global Information Economy," *North Western Journal of Technology and Intellectual Property* 11:7 (2013), p. 683.

63 Article 4 of Shangyong Mima Guanli Tiaoli (商用密码管理条例), "Regulation of Commercial Encryption Codes," State Council, Directive No. 273, Oct. 7, 1999, China, <http://newmedia.cityu.edu.hk/cyberlaw/gp3/pdf/law_encryption.pdf>.

64 Ibid.

containing encryption technology is restricted in China because of the focus on protecting information security, strengthening commercial encryption management, and safeguarding national security interests.[65] China has pursued a policy of favoring the development of domestic cryptography systems, for example with the creation of a new Chinese standard for wireless Wi-Fi security (WAPI). This kind of approach could be damaging to international competitiveness since foreign companies hoping to sell wi-fi devices to China would have to co-produce their product with designated Chinese firms.[66]

Furthermore, the WAPI standard raises fear that the domestic cryptography standard would create a functional key escrow system that would allow the Chinese Government easier access to encrypted communications. More recently, China's legislature approved an anti-terrorism law which requires companies to hand over technical information and help with decryption when the police or state security agents demand it for investigating or preventing terrorist cases.[67] This provision has created concern among human rights groups about the Chinese government's increasingly intrusive powers and has also created a warning for international companies that use encrypted technology in China such as Cisco, IBM and Apple, all of which have big stakes there.

Interestingly, multinationals are not the only advocates of more relaxed provisions concerning encryption. The Dutch government, for example, published a position paper in which it "endorses the importance of strong encryption for internet security, for supporting the protection of citizens' privacy, for confidential communication by the government and companies, and for the Dutch economy."[68] The paper also states that

> *"The ability to use encryption strengthens the international competitiveness of the Netherlands, and promotes an attractive climate for businesses and innovation […]. Trust in secure communication and storage of data is essential for the (future) growing potential of the Dutch economy, that mainly resides in the digital economy."*

Although the same technology is an obstacle in legitimate investigations, the Dutch paper calls for a "search for new solutions" and opposes the introduction of backdoors in encryption products. Similarly, the French government has rejected crypto backdoors as "the wrong solution." The Deputy Minister for Digital Affairs Axelle Lemaire, speaking on behalf of the French government, rejected an amendment to the new "Law for the Digital Republic," calling for computer companies to provide backdoors to encrypted systems.[69]

---

65 Yu, Xia and Murphy, Mattew (MMlC Group), "The Regulation of Encryption Products in China," *Bloomberg Law Reports – Asia Pacific* 4:2 (2011), p. 1.

66 This clearly suggests a protectionist tool used by Chinese government to promote domestic technology production.

67 Chris Buckley, "China Passes Anti-terrorism Law That Critics Fear May Overreach," *The New York Times*, December 27, 2015, <https://nyti.ms/1ZvqB5L>.

68 G.A. van der Steur, Minister van Veiligheid en Justitie, H.G.J. Kamp, Minister van Economische Zaken, Brief regering, January 4, 2016.

69 Glyn Moody, "French Government Rejects Crypto Backdoors as the Wrong Solution," *Ars Technica*, January 14, 2016, <https://arstechnica.co.uk/tech-policy/2016/01/french-government-rejects-crypto-backdoors-as-the-wrong-solution/>.

To conclude, in the specific case of cryptography, varying regulations and implementations worldwide are considerable obstacles to information technology and security firms' willingness to expand into new markets. Therefore, multinational firms may suffer from this lack of understanding at the international level.[70] At the same time, the right to privacy is at stake since the only way to protect the privacy of digital information is by encryption.

Is a New Definition Necessary?

This article has argued for a common understanding of the dual-use concept. In this regard, one may wonder if the adoption of a new, global definition may be a fundamental condition to achieve this purpose. Yet, this leads to another question in turn: If export control regime guidelines set the standards for national export controls, are they uniformly implemented by Member States? As this article has shown, they are not. Beyond this, catch-all clauses or different perceptions of a dual-use item, as in the case of cryptography, suggest it is not just a matter of standards. By analogy, the same reasoning may be applied to justify the uselessness of a new common definition of dual-use. There is no room to think that a new definition will lead to a homogeneous and global implementation of dual-use export controls. Inevitably, different interpretations, investigation and enforcement structures, borderline cases, end-user concerns, and levels of information or intelligence among states lead to different export control decisions.

However, if on the one hand the adoption of a new definition is far from being the solution to the current weak international export control system, on the other hand it may be valid and useful to propose a modern and consistent definition that incorporates the different understandings of the concept and reflects the evolution it has undergone. Any new definition proposal should clearly touch on the following: (1) which "items" are to be controlled, (2) which purposive nature, and (3) which scope/security.

For instance, considering the subcategory "items," and the confused way in which they are used by different instruments (see Annex I), dual-use may refer to "item" in the sense of goods, including software and technologies. Moreover, to consider the dual-use concept in the life-sciences, "items" should also refer to "information." However, information should not be interpreted in the *sensu stricto* of "technology," which many lists already refer to. Rather, it should be meant as the information issues related to dual-use arising from research.

In addition, in light of the multiplication of items with uncertain dual-use features (due also to the increasingly blurry lines between civilian and defense technology and industrial bases), and with the multiplication of dual-use items with no predominately military use (e.g., surveillance technology, encryption), a question remains concerning the traditional dichotomy between civil vs. military.

Finally, in view of the dissimilar scopes of several international instruments governing dual-use commerce (see Annex I), a valuable scope to include in the new definition may be "*peaceful and non-peaceful"* in order to comprehend the purpose of every instrument. However, this umbrella definition approach would not take into account the shift from national security interests to human security interests since the concept of peaceful vs. non-peaceful originates

70 In this regard, the DigitalEurope position on the EU-US regulatory cooperation is illustrative.

in the international concept of war and peace. Therefore, given that, (1) the concept of dual-use seems to have shifted from state's concern for security to consideration also of human security (e.g., the EU understanding of dual-use as related to human rights violation; the US understanding of dual-use as related to terrorism), (2) taking into account the dual-use research of concern area, (3) and the case of cryptography which underlines the possible threats to human rights to privacy (therefore to political security), the definition may refer to items which threaten *human security,* used as umbrella concept that includes political security. These are suggestions which aim to open the way for further studies in this direction.

Conclusion

This investigation of legally and politically binding instruments referring to the dual-use concept has demonstrated the lack of a common definition and identified and compared similarities and differences in national understandings of dual-use. The article has analyzed to what extent the international community has confusingly worded the concept of dual-use.

One of the most significant findings is that the concept of dual-use has evolved from state proliferation concerns to encompass also non-state proliferation concerns, thus shifting from national security interests to human security interests. In this regard, the US and EU approach are empirical evidence. On the one hand, the US maintains unilateral controls on a wide range of dual-use items predominantly for anti-terrorism reasons, such as anti-terrorism export controls on 5A992 and 5D992 categories, to which there is no EU equivalent. On the other hand, the EU has shown a human rights approach to the dual-use concept by appealing to Article VIII of the EU Dual-Use Regulation and maintaining ongoing dialogue through regulatory reform discussions within the EU. Although the EU and the US adhere to the same multilateral export control regimes and have a lot in common (i.e., defining dual-use as having both civil and military applications), they employ different approaches when it comes to implementation.

The common denominator for all export controls regimes consists of lists of dual-use items. Nevertheless, the consideration of the case of cryptography has revealed a lack of conformity among these international instruments. This, however, does not imply that lists are not the most practical way to achieve common and objective guidance.

Besides the harmonization of lists and systems, a reconceptualization of dual-use may be useful. There is a need for a modern and consistent definition to incorporate the different understandings of the concept and to reflect the evolution it has undergone, as technology and interpretations are constantly changing. This investigation has paved the way for new studies and literature focused on the meaning itself of dual-use that can benefit the international community.

ANNEX I

Figure 1: Matrix of the terms used to refer to dual-use, articulated in the 3 subcategories of items, and the scope of each instrument.

	ITEMS			SCOPE
	GOODS = Tangibility	**TECHNOLOGY**	**SOFTWARE**	
International Regimes, General	Not formally and directly defined.	General consensus on the meaning of the term when it is used.	Same definition in the dual-use export control systems and regimes 'worldwide.'	
BWC & CWC	Do not refer to these 3 categories but, respectively, to *"the agents, toxins, weapons, equipment or means of delivery specified in Article I of this Convention"* and the *"chemical weapons and related activities."* [71,72]			Prohibition of *chemical and biological weapons* to facilitate general and complete disarmament.
NPT	Article III.2 does not mention any of the 3 categories but only the *"equipment and materials"* which can serve proliferation purposes.			Prevention of wider dissemination of *nuclear weapons* – Development of the applications of atomic energy for peaceful purposes.
Zangger Committee	Designates under the term items *"equipment or material especially designed or prepared for the processing, use or production of special fissionable material."*			Stems from Article II.2 of the NPT. Same objectives.
Nuclear Suppliers Group	Targeting *"certain equipment, materials, software, and related technology* that could *make a major contribution* to a *"nuclear explosive activity,"* an *"unsafeguarded nuclear fuel-cycle activity."* (It does not propose a formal definition of the "equipment" and "materials").	"Specific information required for the *development, production,* or *use* of any item. This information may take the form of *technical data* or *technical assistance."*	"A collection of one or more "programs" or "microprograms" fixed in any tangible medium of expression."	Prevent a *major contribution to a nuclear explosive activity, an unsafeguarded nuclear fuel-cycle activity or acts of nuclear terrorism*.

71 BWC Article III.

72 CWC Article I.

	ITEMS			SCOPE
The Australia Group	*"Materials, equipment, technology and software that could contribute to CBW activities,"* (thus suggesting that the sub-category of "goods" may be further divided between "materials" and "equipment"). However, the control list adopted by this *forum* only refers—without defining it—to the "equipment."			Fulfill the obligations under the CWC and BWC.
Missile Technology Control Regime	*Items* and *equipment* are indifferently used, but they are opposed to technology.	Same definition of NSG.	Same definition of NSG.	Prevent *missile development, production and operation*.
The Wassenaar Arrangement	It does not provide any definition of "goods," though it use the term in the title of its Initial Elements and the section dedicated to the scope of its controls.	Same definition of NSG. Annex I. General Technology Note & General Software Note (ex. Controls do not apply to "technology" "in the public domain," to "basic scientific research" or to the minimum necessary information for patent applications).	Same definition of NSG.	Controlling *military* capabilities
Resolution 1540 (2004)	*Items* refer to *materials* related to the "proliferation of nuclear, chemical or biological weapon and their means of delivery."			In response to *global terrorism* and the risk that *non-state actors* may acquire, develop traffic in or use *nuclear, chemical and biological weapons* and their means of delivery.
EU Regulation 428/2009	"Dual-use items shall mean items, including software and technology, which can be used for both *civil and military purposes*, and shall include all goods which can be used for both *non-explosive* uses and assisting in any way in the manufacture of *nuclear weapons* or other nuclear explosive devices."[73] (It seems that the definition of *items, goods* but also *technology* and *software* as dual-use ones is subjected to both aspects of principles and opportunity).[74] European parliament legislative resolution states: "…for use in connection with a *violation of human rights, democratic principles or freedom of speech* […], by using *interception technologies* and *digital data transfer devices for monitoring mobile phones and text messages* and *targeted surveillance of internet use*, such as via monitoring centers or lawful interception gateways."[75]	Provides a definition similar to the definition provided by the international systems. General Technology Note (GTN), General Software Note (GSN), Nuclear Technology Note (NTN). Despite the existence of a definition at the EU level, the MS have inserted a definition of "technology" in their national implementing legislation. (ex. In the British Export Control Order, technology means information that is "capable"—and not compulsorily "necessary"—to be used for such purposes, which enlarges the possibilities of control).	Same definition of NSG – Annex I. General Software Note (GSN).	Cumulates WA, AG, MTCR and NSG objectives. Effort to extend the original scope to protection of human rights and democratic principles, to torture or other cruel inhuman or degrading treatment or punishment.

	ITEMS			SCOPE
US internal regulations	*The term 'dual- use' is often used to describe the types of items subject to the EAR. A 'dual-use' item is one that has civil applications as well as terrorism and military or weapons of mass destruction (WMD)-related applications.*[76] The term goods is not used. However, an *item* means "commodities, software, and technology."[77] The term commodity is defined as "any article, material or supply except technology and software." (An item shall be reviewed with the light of the Commerce Control List and the provisions of the Regulations.)	*"Basic Scientific Research."* (GTN) – "Experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective." GSN.	Same definition of NSG.	Controlling *terrorism, military or WMD*-related items.
WHO definition of dual-use in life sciences[78]	"Initially used to refer to the aspects of certain materials, information and technologies that are useful in both *military and civilian* spheres. The expression is increasingly being used to refer not only to military and civilian purposes, but also to *harmful misuse* and *peaceful activities*."			From *military and civilian* sphere it extended to *harmful misuse* and *peaceful activities*.

73 Council Regulation (EC) No. 428/2009 of 5 May 2009, Article 2.1.

74 Quentin Michel, Sylvian Paile, Maryna Tsukanova, and Andrea Viski, *Controlling the Trade of Dual-Use Goods- A Handbook*, (Brussels, P.I.E. Peter Lang, 2013), p. 79.

75 Position of the European Parliament adopted at first reading on 23 October 2012 with a view to the adoption of Regulation (EU) No. .../2012 of the European Parliament and of the Council amending Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.

76 US Department of Commerce, "EAR – Part 730, General Information," BIS, May 21, 2015.

77 US Department of Commerce, "EAR – Part 772, Definition of terms," BIS, May 21, 2015.

78 In respect to life sciences research that have dual-use potential, it is useful to the present work to mention at least one reference to it made by an international instrument.

ANNEX II

Figure 2: Overview per Country of Cryptography Laws[79]

COUNTRY	IMPORT CONTROLS	EXPORT CONTROLS	DOMESTIC LAWS AND REGULATIONS
Antigua and Barbuda	X	X	X
Argentina[80]	O		O
Australia	X	X	X
Austria	X	X	X
Bahrain			X
Bangladesh			O
Belarus	X	X	X
Belgium	X	X	X
Brazil	O		O
Bulgaria			
Burma	X	X	X
Cambodia	O		O
Canada	X	X	O
Chile	O		O
People's Republic of China	X	X	X
Colombia	O		O
Costa Rica			
Czech Republic	X	X	O
Denmark	X	X	O
Egypt	X	O	
Estonia	O	X[81]	
Finland	O	X	X
France	X	X[82]	X[83]
Germany	X	X	X
Ghana	O		O
Greece	O	X	X
Hong Kong	X	X	O[84]

Legend: X = Yes; O = No; Blank = no reliable data source found

79 *Cfr.* Bert-Jaap, Koops, "Crypto Law Survey, Overview per country," (February 2013), <www.cryptolaw.org>

80 Argentina has signed the Wassenaar Arrangement, so export controls should be regulated according to the pre-December 1998 Arrangement, including the General Software Note.

81 There are no import controls, but export is controlled along the Wassenaar model.

82 France has signed the Wassenaar Arrangement for *export* controls, with the exception of the (pre- December 1998) General Software Note.

83 France used to restrict the domestic use and supply of cryptography for a long time. This restrictive legislation (authorization and declaration were required for almost all cryptography) was slightly liberalized since 1996.

COUNTRY	IMPORT CONTROLS	EXPORT CONTROLS	DOMESTIC LAWS AND REGULATIONS
Hungary	X	X	X
Iceland			O
India	X		X
Indonesia	O		
Iran			X
Ireland	O	X	X
Israel	X	X	X
Italy	X	X	X
Japan		X	O
Kazakhstan	X	X	X
Kenya	O		O
Kyrgyzstan		O	
Latvia	X	X	O
Lithuania	X	X	O
Luxembourg	X	X	O
Malaysia	O	O	O
Mauritius	O	O	O
Mexico	O	O	O
Moldova	X	X	O
Morocco	X	X	X
Netherlands	X	X	X
New Zealand	X	X	O
North Korea[85]			
Norway	O	X	O
Pakistan			X
Peru	O	O	O
Philippines			O

Legend: X = Yes; O = No; Blank = no reliable data source found

84 There are no regulations on the use of encryption. Crypto products that are to be connected to the public telecoms network, however, must comply with the relevant Telecommunications Authority's network connection specifications.

85 When requested to provide information about its encryption laws, the government of the Democratic People's Republic of Korea stated that they never release such information.

Figure 2: Overview per Country of Cryptography Laws Continued

COUNTRY	IMPORT CONTROLS	EXPORT CONTROLS	DOMESTIC LAWS AND REGULATIONS
Poland	X	X	O
Portugal		X	O
Puerto Rico	O		O
Romania	O		
Russia			O
Rwanda			
Saudi Arabia	O	O	X
Singapore	O	X	O
Slovakia		X	
Slovenia			X
South Africa	X[86]	X[87]	X
South Korea	X	X	X
Spain		X	X
Sweden	O	X	X
Switzerland	O	X	O[88]
Syria			O
Thailand			X
Tonga			X
Trinidad & Tobago			X
Tunisia	X		X
Turkey			
Ukraine	X	X	X
United Kingdom	X	X	X
United States of America	O	X[89]	X
Uruguay	O		O
Venezuela			O
Vietnam	O		

Legend: X = Yes; O = No; Blank = no reliable data source found

86 There are import and export controls for military cryptography. Otherwise crypto import and export is free.

87 Use of encryption is free for commercial or private organizations.

88 Apart from these two specific regulations, there are no domestic crypto regulations.

89 The US has signed the Wassenaar Arrangement, but does not implement the (pre-December 1998) General Software Note and generally maintains stricter controls.