The European Journal of International Law Vol. 31 no. 3
*© The Author(s), 2020. Published by Oxford University Press on behalf of EJIL Ltd.
All rights reserved. For Permissions, please email: journals.permissions@oup.com*

Diagonal Export Controls to Counter Diagonal Transnational Attacks on Civil Society

Herbert Lin[*] and Joel Trachtman[**]

Abstract

Modern geopolitics includes measures short of armed conflict designed to control decision-making in, and action by, target states. One increasingly significant category of these measures involves attacks by foreign states against civil society institutions in target states. Liberal states that seek to protect their civil societies from this interference seek to bolster civil society defences, to determine the origin of and respond to attacks and to deny relevant tools to potential attackers. With the rise of cyberspace, target states using purely territorial measures are increasingly impotent to protect their civil societies from foreign governmental hacking. Denying access to advanced hacking software by antagonist foreign states may assist in protecting target state civil societies. This article explores the possibility of denying hacking tools to potential attackers, identifies some of the problems and proposes a refinement of export controls that will permit greater protection with less disruption of desirable software development.

1 Introduction

A *The Problem of Governmental Hacking of Foreign Civil Society*

In the past decade, cybersecurity has become an increasingly important problem of public policy for nations around the world as the frequency and sophistication of cyberattacks has skyrocketed. Advanced societies have grown dependent on computer

[*] Senior Research Scholar at the Center for International Security and Cooperation at Stanford University, and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution. Email: herbert.s.lin@stanford.edu.

[**] Professor of International Law at The Fletcher School of Law and Diplomacy, Tufts University. Email: joel.trachtman@tufts.edu.
This article was prepared as part of a project on Protecting Civilian Institutions and Infrastructure from Cyber Operations: Designing International Law and Organizations, carried out by the Center for International Law and Governance at The Fletcher School of Law and Diplomacy, with financial support of the Microsoft Corporation and the Hitachi Center for Technology and International Affairs. The authors are grateful for advice and comments on earlier drafts from Ian Johnstone, Susan Landau, Jonathan Zittrain and other participants at the project's conference in September 2018.

doi:10.1093/ejil/chaa053

networks, and are expected to become more so, especially as artificial intelligence and robotic machines become more prevalent. This dependence increases the importance of network security, and increases the magnitude of threats to network security. It increases their asymmetric vulnerability.

We have known for years about the exposure of military and other government institutions to cyberattack, and some progress has been made in identifying international cybersecurity norms to address the application of the *jus ad bellum* and the *jus in bello* to that problem – most prominently in the *Tallinn Manual*. Yet individual citizens, non-governmental organizations (NGOs) (including think tanks, foundations, political parties and universities), private firms and nongovernmental infrastructure like the electric grid (collectively, 'civil society') are also vulnerable, and this may present attractive targets outside the context of armed attack or warfare.[1] Private entities such as Hacking Team[2] or NSO Group Technologies[3] have assisted repressive governments in hacking civil society organizations within and outside the territories of those governments. Liberal states, with more influential civil societies, present a greater target for this type of attack than illiberal states.

Consider the following examples of recent cyberattacks by governments on civil society in other states:

- Operation Aurora (2009): A political and corporate espionage effort that exploited security flaws in e-mail attachments on Gmail, and was also aimed at 34 other companies including Yahoo, Symantec, Northrop Grumman, Morgan Stanley and Dow Chemical.[4]
- Shamoon (2012): A massive cyberattack against the Saudi oil company Aramco (controlled by government), forcing it to shut down the company's internal corporate network, and disable employees' email and Internet access.[5]
- Sony Pictures Attack (2014): A hacker group called 'Guardians of Peace' associated with state agencies in North Korea 'knocked out' computer systems at Sony and leaked confidential data from the film studio. The USA has now indicted a North Korean intelligence agent in connection with this attack, along with the 'WannaCry' attack described below.[6]

[1] See D. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (2018); J. Sciutto, *The Shadow War* (2019).

[2] Greenberg, 'Hacking Team Breach Shows a Global Spying Firm Run Amok', *Wired* (6 July 2015), available at www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok/.

[3] Srivastava and Wilson, 'Inside the WhatsApp Hack: How an Israeli Technology Was Used to Spy', *Financial Times* (*Fin. T.*) (29 October 2019), available at www.ft.com/content/d9127eae-f99d-11e9-98fd-4d6c20050229.

[4] Cha and Nakashima, 'Google China Cyberattack Part of Vast Espionage Campaign, Experts Say', *Washington Post* (*Wash. Post*) (14 January 2010), available at www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html.

[5] Perlroth, 'In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back', *New York Times* (23 October 2012), available at www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

[6] Peterson, 'The Sony Pictures Hack, Explained', *Wash. Post* (18 December 2014), available at www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

- A group called the 'Cyber Caliphate' (2015) brought down channels, networks and social media handles of the French broadcaster TV5 Monde.[7]
- Russian government agents attacked the Democratic National Committee (DNC) in connection with the US elections in 2016.[8]
- The WannaCry ransomware attack (2017) targeted computers running 'legacy' Microsoft Windows operating system and sought ransom payments in Bitcoin. Targeted systems included the UK National Health Service, Nissan UK, Renault, electrical power distribution systems in India and universities in China.[9]
- German think tanks (2017) associated with the country's two major political parties, the Konrad Adenauer Foundation (KAS) and Friedrich Ebert Foundation (FES), have been the subject of cyberattacks.[10]
- The Petya ransomware/wiper (2017) attacked the advertiser WPP, food company Mondelez, legal firm DLA Piper and Danish shipping and transport firm Maersk.[11]
- Reports that Russian government agents (2019) began attacks on European elections in 2018 and 2019.[12]

These and other attacks span a broad range and take different forms. Sometimes they destroy data and computer systems. Sometimes they steal (exfiltrate) data that should be confidential. Sometimes they compromise the availability of computer or network resources for legitimate users. Taken as a whole, they increasingly threaten the foundations of liberal society, insofar as they extend political and civil society manipulation transnationally from a foreign state to the political and social order of a target state. But unlike military, other sensitive governmental or critical infrastructure targets, these targets are often not well protected against attack.

B *Protecting Civil Society*

Some steps can be taken to help protect civil society against such attacks. For example, it may be possible to restrict the availability of hacking software to potential attackers through the use of export controls. Ordinary export controls based on the intended

[7] Corera, 'How France's TV5 Was Almost Destroyed by "Russian Hackers"', *BBC* (10 October 2016), available at www.bbc.com/news/technology-37590375.

[8] Barret, 'DNC Lawsuit Reveals Key Details About Devastating 2016 Hack', *Wired* (20 April 2018), available at www.wired.com/story/dnc-lawsuit-reveals-key-details-2016-hack/.

[9] Fung, 'How to Protect Yourself From the Global Ransomware Attack', *Wash. Post* (15 May 2017), available at www.washingtonpost.com/news/the-switch/wp/2017/05/15/how-to-protect-yourself-from-the-global-ransomware-attack/.

[10] Shalal, 'Germany Confirms Cyber Attacks on Political Party Think Tanks', *Thomson Reuters News* (27 April 2017), available at https://news.trust.org/item/20170427170644-3rav8.

[11] Henley, '"Petya" Ransomware Attack Strikes Companies Across Europe and US', *The Guardian* (27 June 2017), available at www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe.

[12] Delcker, 'Ex-NATO Chief: Russia to Launch "Major" Effort to Meddle in European Election', *Politico* (15 February 2019), available at www.politico.eu/article/russia-eu-election-meddling-major-effort/.

destination of exported items, applied to hacking software, may excessively limit software development and even response to attack. On the other hand, re-designed export controls that focus on the 'personality' and 'character' of individual recipients of the software, more than the destination territory, may be able to provide useful protection at reduced collateral cost.

1 *Diagonal Transnational Attack and Response*

Cyberattack by a foreign government on non-government targets may be understood as a type of diagonal transnational attack, compared to a vertical attack by a government on its own citizens, or a horizontal attack by one government against another. In a sense, it represents a novel kind of transnational conflict, in which the attacks by one government against a target state's civil society transcend the target state government. While this type of attack existed prior to the growth of cyberspace, it is greatly facilitated, and made more dangerous, by pervasive cyberspace connections. One strategy in response would be to isolate the target state from foreign networks, but this would be overbroad, and may create damages greater than its benefits.

Foreign states may wish to attack civil society organizations in a target state either because those civil society organizations carry out functions that adversely affect the foreign state, or because the civil society organization advances a policy in its home state that is detrimental to the foreign state. This is a kind of diagonal statecraft that is facilitated in modern contexts by the cross-border penetration allowed by cyber networks. In this article, we focus on attacks against civil society because government institutions can erect strong defences, while civil society institutions often invest less in defence, and are seen as 'soft' targets.

This article evaluates a somewhat symmetrical potential response to diagonal attacks. This response could make export restrictions on hacking software less burdensome and more effective, by taking advantage of the independent role of private sector entities within the attacking state. In both the offensive and defensive aspects, states are separated from their civil societies, and a diagonal attack may be met with a hybrid horizontal-diagonal response. As illustrated in Figure 1 below, in the offensive case, direct action is taken by an attacking state against a target state's civil society, and in the defensive case, 'validated user' regulation is used to allow exports of software to segregated validated software developers within the territory of potential attacking states, while reducing the possibility of use by the potential attacking state. As we discuss throughout this paper, this hybrid horizontal-diagonal response allows for greater dissemination of software, with less risk of abuse.

It is not mere aesthetic symmetry that recommends a diagonal response to a diagonal attack; rather, it is the eroding monopoly of the state on territorial power. On the one hand, the target state lacks the territorial power to defend its civil society institutions from cyberattack, while on the other hand, the potential attacking state can be induced to give up territorial power, and can reasonably effectively do so, in order to promote its domestic software industry, and to itself remain an acceptable host country for the transnational software development network.

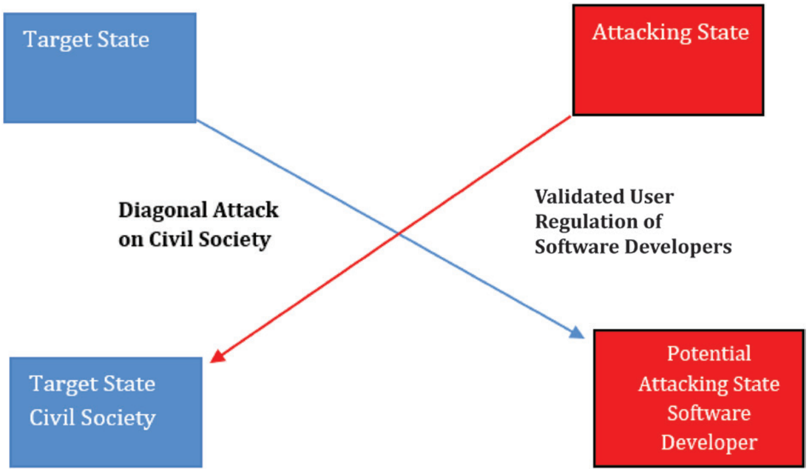
Target State
Attacking State
Diagonal Attack on Civil Society
Validated User Regulation of Software Developers
Target State Civil Society
Potential Attacking State Software Developer

Figure 1: *Diagonal attack and controls*

2 *The Role of Export Controls*

Some states have sought to use export control mechanisms to reduce the availability to governments of the instruments needed to conduct cyberattacks on civil society. However, when the instruments in question consist of software, the use of export controls is often both difficult and controversial. The use of export controls to restrict movement of software is made difficult by the fact that software moves across borders at essentially zero cost, and software development, management and use occur throughout an effectively borderless, and networked, world. The production of software is globally integrated. For these reasons, territorially based export controls on software are extremely difficult to enforce.

It is critical to note that export controls can only constitute a partial response to diagonal cyberattacks, due to (i) the real possibility that export controls can be evaded, especially in the software field, and (ii) the possibility of indigenous development of effective hacking software in states like China, Iran, North Korea and Russia. However, export controls may assist in reducing the capabilities of these and other potential attackers, and so the scope of vulnerability. The question that this article responds to is whether controls can be designed in such a way as to provide a useful measure of protection while presenting a reasonable, and acceptable, burden on software development, including the development of defensive measures against cyberattack.

It is important to note that concerns have also grown regarding the use of intrusion software by governments to attack and to undermine the human rights[13] of their own citizens: 'vertical' attacks.[14] Export controls regarding intrusion software have

[13] Cohn, 'Export Controls: The New Frontier in Cybersecurity?', *Microsoft EU Policy Blog* (13 April 2017), available at https://blogs.microsoft.com/eupolicy/2017/04/13/export-controls-the-next-frontier-in-cybersecurity/.

[14] The European Commission sought to add human rights as a basis for these export controls in 2017. See Clarke, 'Cyber-Surveillance Technology and Export Control: Changes on the Horizon, Part 1', *Insights* (15 February 2017), available at www.osborneclarke.com/insights/cyber-surveillance-technology-and-export-control-changes-on-the-horizon-part-1/.

largely focused on these types of human rights violations, with the implicit assumption that human rights obligations are owed by governments to their own citizens, and not 'extraterritorially' (or perhaps 'extra-nationally') to citizens of other states. As a practical matter, of course, a state with access to intrusion software can use it against its own citizens or against those of other states. However, potential target states or their allies have a greater claim to restrict access to these tools where the tools will be deployed by attacking foreign states against the citizens of those controlling states: when they are used to compromise human rights extraterritorially.[15]

At the core of the intrusion software problem is the technical fact that intrusion software is both a sword and a shield. As a sword, intrusion software can be used by malicious parties for nefarious purposes. As a shield, the ability to transfer intrusion software to legitimate security researchers and multinational firms increases their legitimate cyber defensive capabilities. Thus, an export control mechanism that can distinguish between these roles, on the basis of the credentials and undertakings of the recipients, is essential.

It is also true that software development, including cybersecurity, is a growing field of economic activity, as well as a growing field of transnational production. Demand for software products, including cybersecurity products and services, is steadily on the rise. Moreover, software development is knowledge-intensive rather than capital-intensive, a fact that puts the development of a software industry within reach of capital-poor states. Export control regimes that limit the globalization of software development will impair global production, with important effects on the scope for economic development. Again, an appropriately tailored export control regime might be able to minimize this detriment.

3 *Moving From Territoriality to Personality*

It is noteworthy that current export control law in the United States and elsewhere includes restrictions not just on the transfer of certain commodities or technologies to particular states, but also to particular persons. For example, software and technical data disclosed to a foreign national, even if present within the United States, can be a 'deemed export'.[16] In other words, the conventional formulation of export controls focusing on the destination state alone has already been modified in some limited dimensions.

The possibility of greater focus on the recipients of controlled intrusion software is the basis for this article's proposal for improvement in the existing export control regime relating to hacking software. In this article, we examine some existing regimes that focus on the nature of the recipient, rather than the geographic destination per

[15] Note also that intrusion software is used by national law enforcement agencies, and by intelligence agencies, for legitimate purposes. For example, the intrusion may be carried out pursuant to a procedurally satisfactory search warrant. So, not all use of intrusion software against citizens is illegitimate, and export controls must distinguish between exports to governments that will use intrusion software only for legitimate purposes and those that will not.

[16] Scope of the Export Administration Regulations, 15 CFR § 734.13 (2016).

se. We explore the possibility of developing a regime for combining agreement on controls with agreement on verified users (VUs). Since the goal, as expressed above, is to keep certain tools out of certain state hands, transfer to these VUs must be conditioned on agreement by the relevant states that have legal or physical authority over the VU to respect the VU's responsibility to hold the controlled technology in confidence, without governmental interference. Once we develop these substantive rules, we focus on the structure of an international legal regime, including possibly a revised Wassenaar Arrangement for coordination among states, to administer, modify and enforce the rules, and the political and legal conditions for achieving such a regime.

4 *Structure of the Article*

In Section 2, we review the role of hacking software proliferation in empowering foreign states to attack civil society in target states, and examine existing export control rules and proposals. Section 3 provides our proposed public-private response, establishing 'verified users' in otherwise untrusted states as segregated enclaves to which hacking software can be exported. Verified users are to be identified based on due diligence investigation, contractual commitments, continuing monitoring and host state agreement. This allows the relaxation of territorially based export controls, promoting greater dissemination of software so as to promote free flow of knowledge and commerce, while maintaining security. We evaluate the two-level basis for firms and states accepting this type of verified user regime, and the basis for expecting states and users to comply with this type of regime. Section 4 concludes.

2 Hacking Software Proliferation and Export Controls

In this section, we explore the problems with the existing regime, which include definitional problems that are plagued by overbreadth and under-inclusiveness, as well as problems of breadth of coverage and enforcement.

A *Can We Define Hacking Software?*

At the core of the problem is the difficulty in defining a restricted category of hacking software, and the fact that the same software that is dangerous is also, in other uses, benign and even protective against attack. Therefore, export controls on hacking software often also operate as limits on the scope and efficiency of global development chains for software generally, and cybersecurity software, including software to respond to particular vulnerabilities identified only upon attack, in particular.

The main international forum for discussion of restrictions on export of hacking software is the Wassenaar Arrangement (WA), an intergovernmental group of 42 mostly Western states. In 2013, parties to the WA agreed to export control provisions related to intrusion software, but these proposed controls have raised important concerns regarding their effectiveness, costs and adverse effects on security, and are still subject to contention. The definition of intrusion software currently used by the WA is as follows:

> 'Software' specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures', of a computer or network-capable device, and performing any of the following:
>
> a. The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or
>
> b. The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.[17]

Note, however, that the WA does not call for controls on intrusion software per se (if it did, such software would be less available for 'white hat' uses that support cybersecurity efforts); rather, it controls '"software" specially designed or modified for the generation, command and control or delivery of "intrusion software"'.[18] (For convenience, we refer to this category of software as 'intrusion-related software'.) This dual structure, proposed by the government of the United Kingdom in order to address human rights and security concerns,[19] was intended to avoid excessive constraint on innocent research into flaws, prevention and remediation.

There are a number of difficult technical issues, as well as conceptual issues, involved in these definitions. 'Intrusion software' could include tools that legitimate software developers and cybersecurity professionals may use, such as tools for penetration testing, malware research, vulnerability scanning and security engineering, among others.[20]

It turns out that the good guys use the same tools as the bad guys, though not necessarily in the same ways. And the good guys often involve multinational firms with offices in multiple states, as well as foreign nationals, working with handoffs around the clock. So, innocent intra-corporate sharing, as well as innocent sharing with clients or colleagues, will require export licences that may take weeks to obtain. This may delay response to attacks. One expert observes: 'The WA as written would require export control licences for nearly anyone involved in defensive security activities involving an export of, for example, command and control software and technology

[17] Wassenaar Arrangement Secretariat, 'Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, List of Dual Use Goods and Technologies and Munitions List' (December 2017), available at www.wassenaar.org/app/uploads/2019/consolidated/2017-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf.

[18] *Ibid.*

[19] Wassenaar Arrangement Secretariat, 'Public Statement: 2013 Plenary Meeting', in *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* (December 2017) 53, available at www.wassenaar.org/app/uploads/2019/consolidated/WA_Public_Docs_Vol_IV_Background_Docs_and_Plenary-related_and_other_Statements.pdf.

[20] Goodwin, Griffin, Peltier and Walton, 'Rethinking Intrusion Software.: Ideas for a More Sustainable Approach', *Microsoft Cybersecurity* (2016), available at www.microsoft.com/en-us/cybersecurity/content-hub/rethinking-intrusion-software.

shared in taking down a botnet attack in real time.'[21] The conclusion: 'people who defend and protect computer networks need access to the exact same tools and information that attackers use.'[22] Furthermore, the people who are involved in defensive and remedial efforts are not concentrated in a single country.

Most intractably, certain more general system administrative tools might fall within this definition. Bratus, Locasto and Shubina argue that these categories of controlled software restrict 'the primary known means through which research and engineering progress has been made in all known aspects of software, including security'.[23] These means are 'automation of generation and operation of software elements'. Often legitimate program features will need to be designed to 'defeat protective countermeasures', with the result that these legitimate features will be caught up in the definition of intrusion software. Similarly, software that automatically identifies vulnerabilities of the kind utilized by intrusion software, or 'exploits', would ordinarily be included in legitimate software verification programs. According to these commentators, the definition of controlled items in this field remains unacceptably, and hopelessly, overbroad.

For these reasons, in 2015, after the US Bureau of Industry and Security published proposed rules for implementing the 2013 revised WA controls,[24] industry groups and civil society groups objected to the apparent unintended limits on cross-border vulnerability research.[25] The cybersecurity industry community argued that these export controls would stifle both research leading to improved security, and coordination of response to attack. In addition, while the WA rules excluded 'zero day flaws' – actual identified vulnerabilities in systems – from control, the US proposal included them.[26] Restrictions on transmission of zero day flaws would impede security coordination, as well as the ability to identify flaws through 'bug bounties' by which legitimate companies pay bounties for disclosure of zero day flaws in their systems.

In response to these objections, at the December 2017 WA meeting, the USA sought exceptions to export controls on intrusion software for use in research. These modifications were designed to clarify that technologies 'exchanged for vulnerability

[21] Moussouris, 'Serious Progress Made on the Wassenaar Arrangement for Global Cybersecurity', *The Hill* (17 December 2017), available at https://thehill.com/opinion/cybersecurity/365352-serious-progress-made-on-the-wassenaar-arrangement-for-global.

[22] Cross, 'New Changes to Wassenaar Arrangement Export Controls Will Benefit Cybersecurity', *Forbes* (16 January 2018), available at www.forbes.com/sites/forbestechcouncil/2018/01/16/new-changes-to-wassenaar-arrangement-export-controls-will-benefit-cybersecurity/#24a2f3ba5ed6.

[23] Bratus, Locasto and Shubina, 'Why Wassenaar Arrangement's Definitions of "Intrusion Software" and "Controlled Items" Put Security Research and Defense at Risk', *Usenix* (23 July 2014), available at www.usenix.org/system/files/login/articles/wassenaar.pdf.

[24] US Department of Commerce, Bureau of Industry and Security, 'Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items' (20 May 2015), available at www.gpo.gov/fdsys/pkg/FR-2015-05-20/pdf/2015–11642.pdf.

[25] Ruohonen and Kimpa, 'Updating the Wassenaar Debate Once Again: Surveillance, Intrusion Software, and Ambiguity', 2 *Journal of Information Technology and Politics* (2019) 169.

[26] Fidler, 'Proposed U.S. Export Controls: Implications for Zero-Day Vulnerabilities and Exploits' (10 June 2015), available at www.lawfareblog.com/proposed-us-export-controls-implications-zero-day-vulnerabilities-and-exploits.

disclosure or cyber incident response purposes are not controlled, and updates or upgrades are not controlled', so long as they themselves are not intrusion software.[27] These modifications address important elements of the concerns expressed by the software community about allowing legitimate defensive operations, both before and after an incident. However, they depend on confirmation of the purpose of transfer.

B *Existing Export Control Regimes*

Assuming that there are alternative sources of intrusion technology, then export controls present a cooperation problem at both national and international levels. Cooperation is implicit in the idea of export controls: government intervenes to require producers to restrict their sales in order to promote the common good. National government addresses the cooperation problem at the national level; international law or informal regimes address the cooperation problems at the international level.[28]

At the national level, the idea of an export control ordinarily requires governmental restriction of private activity: governments prohibit unlicensed export of restricted technology. Private persons could, in theory, develop their own set of export controls, and if those controls could operate effectively, they might pre-empt the need for governmentally imposed controls. For example, in April 2018, a group of largely western technology companies agreed to a 'Cybersecurity Tech Accord' that, among other things, informally commits them not 'to help governments launch cyberattacks against innocent citizens and enterprises from anywhere'.[29]

However, even if the software industry as a whole would benefit from export controls on intrusion software, individual software companies would have incentives to avoid accepting, or to defect from, an industry-agreed rule, and it does not appear that there are sufficient market-based incentives to adhere or to comply. While a contractual agreement among relevant suppliers could reduce problematic transfers of software, it may be difficult to induce a sufficient number of suppliers to participate or to enforce their compliance, and participation may raise competition law issues in some jurisdictions. At the national level, this is a public goods cooperation problem, and a main role of national government is to solve it through legal rules.

Of course, different governments will have different incentives in relation to export controls on intrusion software. It should be noted, and highlighted, that export controls may not be able to address indigenous intrusion software capabilities in countries like China, Iran, North Korea or Russia. However, export controls may reduce these capabilities, and would have greater effectiveness on countries with less robust cyber capabilities. More generally, governments of states with the most politically important

[27] US Department of Commerce Bureau of Industry and Security, 'FAQs', (2019), available at www.bis.doc.gov/index.php/policy-guidance/faqs. See also Waterman, 'The Wassenaar Arrangement's Latest Language is Making Security Researchers Very Happy', (20 December 2017), available at www.cyberscoop.com/wassenaar-arrangement-cybersecurity-katie-moussouris/.

[28] See, e.g., J. P. Trachtman, *The Future of International Law: Global Government* (2013).

[29] Cybersecurity Tech Accord, 'Cybersecurity Tech Accord' (April 2018), available at https://cybertechaccord.org/accord/.

civil society institutions – generally liberal governments – and on the other hand, the greatest intrusion software capability – technologically advanced states – are more likely to support controls, provided that they can be designed to avoid excessive restrictions. Governments of states with less important civil society institutions, on the one hand, and less indigenous capability to produce effective intrusion software, on the other hand, would generally oppose controls.

If the goal were to completely prevent transfers of intrusion software, the international 'intrusion software non-proliferation game' could be modelled as a weakest link public goods game[30] in which, unless all of the potential producers of intrusion software comply, the public good of total restriction is not produced. However, we may specify a more modest goal, which is to reduce the overall availability of intrusion software, to deny transfer of the most sophisticated technology for intrusion to the more advanced potential attacking states and to deny transfer of intrusion technology to the less advanced potential attacking states. In this context, non-proliferation is an 'aggregate effort public good', similar to climate change, in which some contributions, even if not totally effective, are helpful in reducing the overall problem.[31]

The WA, initially designed for physical dual use goods, is designed to partially address this cooperation problem. We describe it, and its limitations, below, and then briefly describe the US and EU export control regimes for intrusion software.

C *Wassenaar Arrangement*

Under the WA, participating states have agreed to maintain, through national rules, export controls on items included in the WA control lists. Each participating state retains formal discretion to restrict exports or to allow them. To be clear, the WA is a coordinated list of items that its members plan to, and on a non-legally binding basis agree to, subject to national export controls. In addition, members are required, on a non-legally binding basis, to report transfers or denials of transfers of certain controlled dual-use items.[32]

The WA is not a treaty, but instead operates as a 'soft law' commitment among its member states.[33] In that way, it is similar to the Basel Committee bank capital accords, the Codex Alimentarius and other non-legal rules. The fact that these rules do not impose formal legal requirements under international law does not mean that they do not have effects on state behaviour. But the effects operate at the political or informal level in international relations.

[30] See Hirshleifer, 'From Weakest-Link to Best-Shot: The Voluntary Provision of Public Goods', 41 *Public Choice* (1983) 371.

[31] See Bodansky, 'What's in a Concept? Global Public Goods, International Law, and Legitimacy', 23 *European Journal of International Law* (*EJIL*) (2012) 651.

[32] Wassenaar Arrangement, 'What is the Wassenaar Arrangement?' (20 December 2017), available at www.wassenaar.org/the-wassenaar-arrangement/.

[33] The constitutive document for the Wassenaar Arrangement is the Guidelines and Procedures, including the Initial Elements, the latest version of which is December 2016 (the 'Initial Elements'). See 'The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Initial Elements' (11–12 July 1996), available at www.wassenaar.org/docs/IE96.html.

Because the WA is not binding international law, and because it does not have a formal process of interpretation and dispute settlement, different states apply it with different scopes and degrees of effectiveness. By comparison, the Cold War predecessor regime of the WA, the Coordinating Committee for Multilateral Export Controls (COCOM), included a rule that exports of certain sensitive items by any member state would require prior notification to the other members, and were subject to veto by any member.

The WA includes 42 states,[34] including all of the member states of the EU. The WA notably includes Russia, but, also notably, excludes a number of states with strong software capabilities, including Brazil, China, Iran, Israel, North Korea, Pakistan, South Korea and Taiwan (although some of these states unilaterally adhere to WA restrictions). The WA also encourages voluntary adherence to its standards by non-member states. The WA control lists were first established in 1996 and have been revised annually thereafter, by negotiation among the members. Decisions regarding what to include on the control list are made by consensus. The WA does not directly include private sector participation, and there seems to be wide agreement that the US administration failed adequately to obtain private sector input before accepting the 2013 Wassenaar intrusion software provisions.[35]

While much of the world's intrusion software capability is covered by the WA member states, and other states that adhere to its standards, certain non-compliant states have the capability to produce effective intrusion software. Indeed, the more successful a 'cartel' arrangement such as the WA is, the greater the incentives to defect, or simply to avoid accepting its obligations. So, in order to have the most effective regime possible, movement towards universal membership among software capable states, or at least universal compliance among those states, will be attractive. Of course, membership does not necessarily indicate compliance. And as the regime grows more effective, it will need greater inducements to comply and to remain part of the regime, in order to overcome the increasing attractions of defection. However, incremental benefits may be produced by a regime that does not include universal membership.

D *United States*

The US regime for export controls is administered by the Bureau of Industry and Security (BIS) of the Department of Commerce, under the Export Administration Regulations, including the Commerce Control List of Dual-Use Items (CCL). These regulations have the force of law.

[34] As of 23 November, 2019, the 42 members of the Wassenaar Arrangement were: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom and United States.

[35] Osborne, 'Wassenaar Arrangement: When Small Words Have the Power to Shatter Security', *ZDNet* (4 April 2017), available at www.zdnet.com/article/wassenaar-arrangement-when-wording-may-break-the-us-security-industry/.

In 2015, the BIS proposed to incorporate the 2013 WA agreement by adding the relevant references to the CCL. The proposal, while requiring licences for all other destinations, proposed 'favorable review' if 'destined to a U.S. company or subsidiary not located in Country Group D:1 or E:1 [specified countries less trusted or subject to embargo[36]], foreign commercial partners located in Country Group A:5 [countries more trusted], or government end users in Australia, Canada, New Zealand or the United Kingdom [with the US, the "Five Eyes"] .... Note that there is a policy of presumptive denial for items that have or support rootkit or zero day exploit capabilities'.[37]

Because of private sector criticism in response to the 2015 implementation proposal, at the time of this writing the USA has not yet implemented WA intrusion-related software restrictions, nor has it implemented more recent WA exceptions for 'vulnerability disclosure' and 'cyber incident response'.

E *European Union*

The EU export control regime governs export controls for all EU member states, pursuant to Regulation 428/2009, amended by Regulation 2016/1969.[38] Member states are permitted to impose more stringent restrictions, and Germany has done so with respect to intrusion software.[39] The existing EU controls generally track the WA definitions.

In 2016, EU controls in this area were proposed to be revised.[40] 'The draft regulation introduces the new concept of "human security" to export controls, to prevent the human rights violations associated with certain cyber-surveillance technologies.'[41]

[36] Bureau of Industry and Security, 'License Exceptions: Supplement No. 1 to Part 740', 24 February 2020, available at www.bis.doc.gov/index.php/documents/regulation-docs/452-supplement-no-1-to-part-740-country-groups/file.

[37] US Department of Commerce, 'Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items' (20 May 2015), available at www.federalregister.gov/documents/2015/05/20/2015–11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items. According to a whitepaper published by McAfee, 'rootkit is a term commonly used to describe malware – such as Trojans, worms and viruses – that actively conceals its existence and actions from users and other system processes'. See 'Rootkits, Part 1 of 3: The Growing Threat', *McAfee* (2006), available at https://web.archive.org/web/20060823090948/http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_akapoor_rootkits1_en.pdf.

[38] See Commission Delegated Regulation 2016/1969, OJ 2016 L 307/1; Bromley, 'Export Controls, Human Security and Cyber-Surveillance Technology: Examining the Proposed Changes to the EU Dual-Use Regulation' (December 2017), available at www.sipri.org/sites/default/files/2018-01/sipri1712_bromley.pdf (last visited 15 March 2020).

[39] Verordnung der Bundesregierung Vierte Verordnung zur Änderung der Außenwirtschaftsverordnung [Regulation of the Federal Government: Fourth Regulation amending the Foreign Trade Regulations], 17 July 2015, Elektronischer Bundesanzeiger [eBAnz] at 28 2018 VI (Ger.).

[40] European 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)' (28 September 2016), available at www.europarl.europa.eu/doceo/document/A-8-2017-0390_EN.html#title2.

[41] European Parliament, 'Review of Dual – Use Export Controls' (12 January 2018), available at www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI%282016%29589832_EN.pdf.

'The proposal sets out a two-fold approach, combining detailed controls of a few specific listed items with a "targeted catch-all clause" to act as an "emergency brake" in cases where there is evidence of a risk of misuse.'[42] 'The targeted catch-all control applies 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.'[43] This approach attempts to mitigate some of the potential under-inclusiveness in the definition of intrusion-related software subject to control. However, on 5 June 2019, the EU Council determined not to proceed with these hacking software restrictions.[44]

F *Limitations of the Existing Regime*

The existing regime has a number of limitations that make it unlikely to be effective in avoiding transfers of intrusion software capabilities. First, it only covers a limited number of countries. Second, the countries that are covered have different interpretations of the controls, and different levels of enforcement rigour. Third, the definitions of controlled software are, as discussed below, overbroad and under-inclusive in important respects. Fourth, the institutional structure does not provide for effective international enforcement. The proposal developed below is intended to address these limitations.

3 Toward Relaxation of Controls for Verified End Users

Of course, if all transferees could be trusted to refrain from malicious use of intrusion software, there would be no need for export controls at all. The definition of controlled software thus interacts with the definition of permitted transferee. That is, with a broad group of permitted transferees – a broad group that has been vetted for reliability – it is less likely that a broad definition of controlled software will result in export controls on legitimate transfers. Given the difficulty in developing a narrow definition of controlled software, it seems worthwhile to consider a broadened group of permitted transferees: one that may include transferees located in countries that might not otherwise be permitted destinations. The existing regime, as described above, focuses largely on territorially defined destinations; our proposal suggests focusing on the characteristics of the transferee.

[42] European Commission, *supra* note 40, at 6.

[43] *Ibid.*, at 11. See Bohnenberger, 'The Proliferation of Cyber-Surveillance Technologies: Challenges and Prospects for Strengthened Export Controls', 3 *Strategic Trade Review* (2017) 81, at 81.

[44] *See* Moßbrucker, 'EU States Unanimously Vote Against Stricter Export Controls for Surveillance Equipment', *Netzpolitik* (16 July 2019), available at https://netzpolitik.org/2019/eu-states-unanimously-vote-against-stricter-export-controls-for-surveillance-equipment/.

A *Intra-Company Transfers and Transfers to Private Sector End Users*

There are some precedents for our proposal. As discussed above, the USA proposed implementation of the 2013 Wassenaar controls on hacking-related software included 'favorable review' for exports to a US company or subsidiary not located in certain less-trusted states.[45] While this posture would evidently assist in reducing the restrictive aspect of hacking software controls, it is limited to certain states, and continues to require review.

More specifically, under US export controls, licence exception ENC[46] is available to authorize export without a licence to any country (except certain countries designated as terrorism-supporting or embargoed countries) if the item is being exported either (i) to a subsidiary of a US company, including to foreign nationals who are employees, contractors or interns of a US company or its subsidiaries, for internal company use; or (ii) to private sector end users, headquartered in what is defined as a 'Favourable Treatment Country' (NATO countries and certain other closely allied countries)[47] for internal development or production of new products. This exception serves as an example of an end user-based exception to export controls.

In addition, the BIS maintains a validated end user (VEU) facility, under which a transferee in India or China may be approved in advance.[48] It is worth quoting in full the regulatory standard for approval of a VEU:

> In evaluating an end user for eligibility under authorization VEU, the ERC [End-User Review Committee] will consider a range of information, including such factors as: the entity's record of exclusive engagement in appropriate end use activities; the entity's compliance with U.S. export controls; the need for an on-site review prior to approval; the entity's capability of complying with the requirements of authorization VEU; the entity's agreement to onsite reviews by representatives of the U.S. Government to ensure adherence to the conditions of the VEU authorization; and the entity's relationships with US and foreign companies. In addition, when evaluating the eligibility of an end user, the ERC will consider the status of export controls and the support and adherence to multilateral export control regimes of the government of the eligible destination.[49]

While this program has been subject to criticism,[50] and has not expanded beyond India and China, it may serve as a model for expansion of the scope for international regulatory cooperation between exporting states and importing states, in order to facilitate controlled exports. We discuss how a modified program might address some of the concerns about intrusion software below.

[45] See *supra* note 37.

[46] For 'encryption', see Encryption Commodities, Software and Technology (ENC), 15 CFR § 740.17 (2018).

[47] License Exception ENC Favorable Treatment Countries, 15 CFR Appendix Supplement No. 3, Part 740 (2018).

[48] Authorization Validated End-User (VEU), 15 CFR § 748.15 (2018).

[49] *Ibid.*

[50] See Government Accountability Office, 'EXPORT CONTROLS: Challenges with Commerce's Validated End-User Program May Limit Its Ability to Ensure That Semiconductor Equipment Exported to China Is Used as Intended' (25 September 2008), available at www.gao.gov/products/GAO-08-1095.

As described above, there are several problems with the existing export control regime for intrusion software. One problem is that the specification of the controlled software is overbroad, but this problem would be ameliorated substantially if the universe of licence-free transferees, or transferees that could be licensed generally and in advance, could be expanded. The ENC and VEU programs provide some models for such expansion. What if affiliated companies, other companies that cooperate on software development and even customers, including law enforcement agencies, could be approved in advance as transferees of the controlled intrusion software? This could be done on three conditions:

- First, it would be necessary to perform a due diligence investigation of these transferees, including their internal safeguards and end use of the products, and for the transferees and their employees to contract not to disclose the software in violation of the exporting country's export control laws.
- Second, these transferees would be required to agree to monitoring and auditing of their activities in connection with the transferred intrusion software, by (a) the exporting country government authorities, (b) private sector agents approved by exporting country government authorities or (c) importing country government authorities approved by exporting country government authorities.
- Third, the importing country government would be required to agree to enforce and not to interfere with the transferee's compliance with the transferee's obligations not to disclose the software in violation of the exporting country's export control laws.

This expanded validated user (VU) regime would be designed to provide appropriate assurances that intrusion software would not be used for purposes of attacks on civil society in other states, and presumably in the transferee state as well. Why would transferee states accept this regime? As discussed below, they would be likely to do so in order to allow greater inbound flows of software, including intrusion software, utilized for legitimate purposes, as well as software development expertise. This would bring economic and developmental benefits. Why would transferor states accept this regime? They would be likely to do so in order to allow their firms to export software more readily, as well as to participate efficiently in the global software value chain.

We might ask, can a nonstate entity really resist orders or inducements from host governments or other governments to disclose intrusion software? Much would depend on the ability to induce host governments to make binding commitments to comply with the relevant regime, and to construct a set of punishments for both the disclosing private entity and the government to which the software is disclosed. To the extent that software can be prepared in a way that makes its origin identifiable after an attack, it would be easier to attribute a failure of export controls to a firm and to a government, and to impose punishments. This is a dual attribution problem: the attack needs to be attributed to a government,[51] and the source of the software needs to be attributed to a software firm – if this proposal is implemented, a rogue VU.

The problem of attributing software to the VU is an issue of software provenance.[52] The distinction between source code and object code is important. Source code is the medium in which humans program computers. Source code is readable by humans. Through a process known as compilation, source code is turned into object code, a particular sequence of ones and zeros that are meaningful to the computer and instruct the computer about what to do step by step. Of particular importance is the fact that during the compilation process, information that is meaningful to humans but not to computers is lost. This makes it more difficult to identify the provenance of object code than to identify the provenance of source code.

Assume that the source code of the restricted software is made available to the VU. Suppose that an unauthorized party improperly obtains the restricted software from the VU and incorporates it into a new program, compiles the new program into object code and uses it in an attack. Forensic investigators can usually obtain the offending object code from the targeted computer. The critical question is whether the investigators can determine whether the offending software is associated with the software originally provided to the VU, which presumably is available to the investigator.

Software can be associated with its original creator in two different ways. One set of techniques is based on the identification of characteristic features or aspects of the original software, much as a painting might be associated with a given artist because of a similarity between the pattern of brushstrokes used on that painting and other paintings known to be done by that artist.

For example, software bertillonage is an approach that uses the presence of various software features to reduce the effort of trying to locate a software object within a large corpus of possibilities.[53] Once the entity is determined with high probability to be among a more limited set of known software objects, other techniques can be used to make a more precise identification.

Another approach is called code stylometry,[54] which analyses the style with which software has been written and seeks to associate a software entity of unknown provenance with another specific entity of known provenance.[55] Recent

[51] For an analysis of the attribution problem in this context, see Tsagourias and Farrell, ‘Cyber Attribution: Technical and Legal Approaches and Challenges’, 31 *EJIL* (2020) 941.

[52] A useful perspective on software provenance can be found on the Software Engineering Institute Blog, see Casey, ‘Provenance Inference in Software’, *Carnegie Mellon University, Software Engineering Institute Blog* (3 February 2014), available at https://insights.sei.cmu.edu/sei_blog/2014/02/provenance-inference-in-software.html.

[53] Davies, German, Godfrey and Hindle, ‘Software Bertillonage: Finding the Provenance of an Entity’ (May 2011), at 21–22, available at http://softwareprocess.es/pubs/davies2011MSR-bertillonage.pdf.

[54] Stylometry is the generic name given to techniques that have been used to identify previously unknown works of Shakespeare – these techniques examine the style of an unknown work and determine that it is highly similar in style to those of known works of Shakespeare.

[55] Caliskan-Islam et al., ‘De-Anonymizing Programmers via Code Stylometry, Proceedings of the 24th USENIX Security Symposium’, *Usenix* (August 2015), at 12–14, available at www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-caliskan-islam.pdf.

research has also suggested that by using machine learning techniques, it is more feasible than previously believed to use stylometric techniques on object code.[56] The significance of the latter research is that in the wake of an actual attack, object code may be recoverable while source code will be unavailable, barring very unusual circumstances.

Strictly speaking, neither stylometry nor bertillonage address the provenance problem as it is stated above. The reason is that both techniques (and all other 'brushstroke' techniques) are based on the investigator having access to a corpus with multiple samples of original code. For stylometry, these samples would be authored by the same party. Bertillonage assumes that the new code could have been derived from any one of a large number of code samples and seeks only to narrow a set that must be examined using other techniques. But both techniques are based on the existence of features in code that can be identified. Comparing the original code and the code used in the attack with respect to such features generates measures of similarity that human analysts may be able to use to make a judgment about whether the attacking code was derived from the original code.

A second way of associating software with its creator is to introduce into the original code certain features (here called watermarks) that would be preserved in any reuse of that software.[57] If the attacker incorporates original controlled source code into its own software, examination of the attacker's software would reveal the watermark, thus indicating the true origin of that code. Thus, a violation of the VU agreement could be identified. On the other hand, the attacker's illicit use of code obtained from the VU would almost surely be accompanied by an effort to remove the watermark from the body of code in question, and if the attacker knew about the watermark, it would be able to do so (easily if it knew the details of the watermark, with more difficulty if it only knew of its presence). If only the object version of the original software is made available to the VU, the attacker is likely to have a harder time removing the watermark; this would be a very good reason for the original creator of the software to only provide object code to the VU. On the other hand, it is harder to embed a watermark in object code in the first place.

Watermarking is a cat-and-mouse game. Watermarkers constantly strive for better watermarks – those that will resist attempts at program transformation and other removal techniques – while anti-watermarkers will strive for better ways to remove watermarks.[58]

[56] Caliskan et al., 'When Coding Style Survives Compilation: De-anonymizing Programmers from Executable Binaries' (February 2018), at 18–21, available at http://dx.doi.org/10.14722/ndss.2018.23304.

[57] Dalla Preda and Pasqua, Software Watermarking: A Semantics-Based Approach, *Science Direct* (20 March 2017), available at www.sciencedirect.com/science/article/pii/S1571066117300075.

[58] For a discussion of this struggle (but with the watermarkers winning at this time), see Chen, Wang and Jia, 'Semantic-Integrated Software Watermarking with Tamper-Proofing', 77 *Media Tools and Application* (10 November 2017), https://link.springer.com/content/pdf/10.1007%2Fs11042-017-5373-7.pdf.

B *Need for Broad Agreement: The Carrot and Stick*

If a regime were designed around the enhanced VU approach described above, it would have to address a number of issues. First, which states would be necessary to participate for optimal effectiveness? Second, how would states be induced to adhere and comply, and how would other states be induced to adhere and comply? Third, should it remain, like the WA, in the form of soft rules, or be converted to a legally binding international treaty? Fourth, how would this regime incorporate the views of the private sector, in order to avoid the kinds of errors made in the 2013 WA revisions? Finally, what organizational features, in terms of decision-making, adjudication and executive functions, including research, surveillance and enforcement, should a revised organization have?

1 *Breadth of Membership*

In order for an export control regime to be most effective, states with control over relevant technology would be necessary to participate. At this juncture, effective participation by China, Iran, North Korea and Russia seems unlikely, and so participation would be below the level necessary for maximum effectiveness. The next question, though, is whether some of these less likely states might be persuaded to join and to do so with sufficient effect to be worthwhile. The more important question is whether the achievable level of participation would have sufficient beneficial effects to justify its establishment. Furthermore, it is possible that producers of intrusion technology would relocate to states that do not impose export restrictions, providing another reason why broad adherence is desirable.[59]

2 *Adherence and Compliance Inducements*

(a) Adherence

Given the public good nature of the cooperation problem in connection with intrusion software, it would be useful to procure participation by as many potential source countries as possible. Indeed, the very idea of territoriality implied by the term ‘source country’ is misleading in this context, because software development may be highly mobile due to its technological character. So, broader participation beyond those countries presently enjoying robust intrusion software capabilities may be appropriate.

One way to achieve broad participation would be to link this cooperation with, or incorporate it in, an existing more or less universal organization, such as the United Nations or the World Trade Organization. These organizations would have to approve such link or incorporation through a consensus or unanimous decision, which may

[59] For example, FinFisher, a Swiss firm, is reported to have transferred its intrusion software business to states that are not members of the WA. See Omanovic, ‘Surveillance Companies Ditch Switzerland, But Further Action Needed’, *Privacy International* (5 March 2014), available at https://privacyinternational.org/blog/1502/surveillance-companies-ditch-switzerland-further-action-needed.

Table 1: State interests

Liberal State	Interest	Illiberal State	Interest
Government	1. Commercial opportunity/ growth 2. Cybersecurity	Government	1. Commercial opportunity/growth 2. Cyberattack capability
Industry	Commercial opportunity, including transnational development of software	Industry	Commercial opportunity
Civil society	Cybersecurity	Not represented	Not represented

be difficult to achieve. However, log-rolling has allowed these organizations to make effective changes in the past.

There is a natural and elegant punishment for non-participation: refusal to transfer intrusion software to the non-participating state. There is precedent for this in the Basel Convention on Transboundary Movement of Hazardous Waste, which provides in Article 4(5) that 'a Party shall not permit hazardous wastes or other wastes to be exported to a non-Party or to be imported from a non-Party'.[60] However, some states may find that they would rather maintain freedom to export, while accepting this punishment. Further evaluation of the effectiveness of this mechanism will be necessary in order to determine whether it will be sufficiently effective. Table 1 provides a stylized summary of the qualitative interests of constituencies in liberal and illiberal states, as they relate to hacking software. The magnitude of these interests is impractical to measure. But consider the advantages of the VU approach described above.

From the standpoint of the illiberal state, the VU approach can achieve greater commercial opportunity at the expense of an opportunity to grow its cyberattack capability. However, that opportunity is illusory, because without a VU arrangement, the liberal state would not allow exports and the illiberal state would not have the opportunity for enhanced cyberattack capabilities. Thus, from the standpoint of the illiberal state, the VU arrangement dominates a traditional export control arrangement without a VU.

The VU approach can achieve extended achievement of all of the interests of the liberal state, by promoting commerce and advancing cybersecurity through greater likelihood of participation by illiberal states, without excessive restriction on exports of technology to VUs. Thus, both illiberal states and liberal states are likely to adhere.

If the above approach is insufficient, another approach would be to punish non-participation through other means, including reputational sanctions, as the

[60] Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and their Disposal 1992, 1673 UNTS 126, Art. 4(5).

Organization for Economic Co-operation and Development (OECD) has done in the context of its Harmful Tax Practices program, inducing most tax haven countries to cease some of their worst tax haven abuse practices.[61] This type of linkage-based punishment is at the core of William Nordhaus's proposal for 'climate clubs' using trade sanctions to induce states to join carbon reduction regimes.[62] This structure is not reliant on hard law, or on membership in an international organization, but it has used exposure and international pressure to cause changes in practices. This model, including its surveillance and reporting functions, may be sufficient to support adherence and compliance to export control obligations in connection with intrusion software.

(b) Compliance

The VU arrangement described above would be likely to achieve regime adherence for the reasons expressed above. But would illiberal states adhere, and then violate the rules? Compliance would depend on (a) the likelihood that violation would be detected, the likelihood that violation would be punished and the magnitude of cost of violation, versus (b) the benefits of violation to the violating state. A VU structure should include institutional arrangements to detect and attribute violation, with the needed capacities, including technical capabilities in the stylometry, bertillonage or watermarking techniques described above. The natural punishment for violation would be to cut off future transfers, resulting in a loss of subsequent commercial opportunities. Thus, assuming that detection and attribution of defection is certain, the inducement to comply would equal the inducement to adhere. Given that detection and attribution may be uncertain, in order for a VU structure to meet compliance, and thus to be attractive to liberal state transferors, it must be designed to achieve a sufficient level of detection and attribution capability.

3 *Soft or Hard Rules*

A cooperation regime can utilize formal law or informal rules. Informal rules may be easier for states to adopt, and may provide attractive flexibility.[63] Formal law has the advantage that states may take it more seriously, and it can more readily be subjected to adjudication in order to definitively interpret the definitions, exceptions and thus the obligations. It can therefore be a basis for greater trust. Perhaps counterintuitively, some states may be willing to enter into law of this nature because they can rely more on the performance of other states. Whether a regime is composed of formal or informal rules, it would require some of the same basic features.

[61] See OECD Global Forum on Transparency and Exchange of Information for Tax Purposes, *Tax Transparency 2017: Report on Progress* (2017), available at www.oecd.org/tax/transparency/global-forum-annual-report-2017.pdf.

[62] Nordhaus, 'Climate Clubs: Overcoming Free-Riding in International Climate Policy', 105 *American Economic Review* (2015) 1339.

[63] *See* Shaffer and Pollack, 'Hard v. Soft Law: Alternatives, Complements, and Antagonists in International Governance', 94 *Minnesota Law Review* (2012) 706.

4 *Role of Private Sector*

Any new regime must provide appropriate transparency, notice and comment, and probably a formal role for private sector representatives. This will be important in crafting and interpreting commitments and exceptions in a way that will not have unintended or excessive adverse consequences. One model for private sector participation is purely consultative, and this may be sufficient. Another model would provide for formal private sector participation, along the lines of the International Labour Organization's inclusion of employer and employee representatives.[64] Similarly, in addition to software industry representation, it would be important to also include representatives of the civil society organizations that benefit from protection, in order to ensure that their interests are adequately reflected in crafting commitments and exceptions.

5 *Organizational Functions*

In order to provide for periodic revisions to the 'control list' and other aspects of the relevant obligations, in order definitively to interpret them, in order to engage in research, negotiation support, monitoring, reporting, dispute settlement and enforcement functions, it would be useful to have an international organization. These types of functions could be taken over by the WA. Alternatively, a new UN specialized agency, or the World Trade Organization (WTO), or another organization, could house these functions.

One important organizational function would involve adjudicating determinations of what types of software are covered, and whether relevant exceptions are available.

Another important organizational function would be surveillance and attribution, including addressing the double attribution problem of first, identifying the state from which intrusions emanate, and second, identifying the provenance of the relevant hacking software in order to determine and punish leaking VUs.

4 Conclusion

Territoriality is a decreasingly apposite basis for governmental control. With the rise of cyberspace, target states using purely territorial measures are increasingly impotent to protect their civil societies from foreign governmental hacking. Denying access to advanced hacking software by antagonist foreign states may assist in protecting target state civil societies. Yet to do so may excessively exclude those foreign states from participation in globalized software development, and may prevent software developers from adequately preparing for and responding to attack. By replacing the decreasingly apposite territorial approach to export controls with a more precise personality-based 'dissemination control' that focuses less on the destination territory and more on the

[64] See International Labour Organization (ILO), 'About the ILO', available at www.ilo.org/global/about-the-ilo/lang--en/index.htm.

safeguards from dissemination implemented by the recipient, hacking software proliferation may be inhibited without unnecessary inhibition of software development and response to attack.

While export controls cannot prevent purely indigenous development of hacking software, they can reduce the overall ease of development by antagonist states of hacking software. In order to have sufficient effects to be worthwhile to state participants, a validated user system must have sufficient adherence among software-capable states, and must be able to induce potential antagonist states to accept the regime as the price of access to global software development networks, or through other conditionality. A validated user regime must also be supported by sufficient attribution capabilities to determine not only which attacking state carried out the hacking, but also to determine the provenance of the hacking software.