Developing Controls on Cyber-Surveillance Exports: Civil Society’s Role in Formulating Norms for Cyber Technologies

A Thesis Submitted in Partial Fulfillment of the Requirements for the Award of Honors in Science, Technology and International Affairs

Edmund A. Walsh School of Foreign Service

Georgetown University, Spring 2018

by

Garrett Hinck

Mentor: Dr. Eric Burger
**Acknowledgements**

I want to thank all who aided me in tackling this often obscure, complex topic. Collin Anderson, Kevin Wolf, Stéphane Chardon, Tim Maurer, Mailyn Fidler, Bob Rarog, and Jim Burger all provided invaluable background information and guidance on the key questions to consider. I also want to thank Susan Hennessey, Matthew Kahn and Shannon Togawa Mercer for their insights on my project and for letting me write about export controls for Lawfare.

My thesis adviser, Eric Burger, has been a great guide throughout this project, helping me navigate tasks like filling out IRB forms to shaping my final product for journal submissions. I am grateful for his confidence in my work throughout the project.

I deeply appreciate the work that the STIA faculty put into the honors program, especially Joanna Lewis and Emily Mendenhall. Their guidance has been invaluable, as has their commitment to dealing with my often unfamiliar topic.

And, I am very thankful for all the time and help Martha Finnemore has given me since I first asked to sit down with her last year. I am especially grateful that she agreed to provide feedback on my final draft. I would not have been able to find my niche without it.

Lastly, I want to thank my parents and friends for their support throughout this process. I could not have done it without their confidence and help.
Table of Contents

Abstract 5

I. Introduction 6

II. Background & Analytical Framework 8

III. Emergence of Proposed Surveillance Norms, 2011-2013 16


V. Evolving EU Policies, Putting Norms Into Practice, 2014 – 2017 33

VI. Conclusions 43

Works Cited 46
Tables and Figures

Figures

1. Techniques Used by Norm Entrepreneurs 14
2. Process of Redirecting the “Digital Weapons” Frame Towards Cybersecurity 31

Tables

1. Key Norm Entrepreneurs in the Emergence of Cyber-Surveillance Exports Norms 17
2. Frames, Targets, Issue Linking and Policy Outcomes in the Emergence Phase 31
Abstract
Defining norms — appropriate standards of behavior — for the rapidly evolving landscape of information communications technologies (ICTs) is a seemingly impossible challenge for the international community. But norms for cyber technologies may develop from the activism of civil society, the private sector and independent actors as well as from governments. This article argues that the efforts of NGOs, activists and researchers to regulate ‘cyber-surveillance tools’ are a case of a limited success in creating norms regarding cyber technologies. Cyber-surveillance tools are software products that make use of sophisticated hacking techniques to enable surveillance. Civil society groups have led a years-long campaign to regulate surveillance exports because of human rights concerns about their use by authoritarian regimes.

Using a qualitative analysis of public discourse on cyber-surveillance from key civil society and public officials from 2011 – 2018, this article highlights the role of NGOs and researchers in defining the proposed norm regulating cyber-surveillance exports, framing it to key actors, and influencing governments to apply export controls to these tools. Contrasting the implementation of this norm in the U.S. and the European Union, it finds that differences in the actors who became involved — from cybersecurity researchers to human rights activists — and in which institutions had oversight over implementing export controls led to divergences in how the U.S. and the EU implemented the proposed norm. This analysis draws lessons for effective cultivation of cyber norms by civil society, showing the importance of including technical experts, defining highly targeted norms, and using existing platforms. As developments in ICTs further alter the international arena, efforts to create rules for cyberspace should consider the process by which civil society actors build, shape and advocate for norms for cyber technologies.
I. Introduction

When protestors stormed the headquarters of Egypt’s infamous secret police in the midst of the turmoil of the Arab Spring in early 2011, they discovered evidence that Western companies sold sophisticated hacking software that enabled Egypt’s surveillance state. Among piles of shredded documents, the protestors found contracts from a UK company, Gamma International, offering its “FinSpy” tool, a commercial software system, to the regime to help it track, monitor and arrest dissidents.¹ Forensic analysis of software samples from across the Middle East and elsewhere revealed the global proliferation of Western-developed hacking software products, which came to be known as cyber-surveillance tools.² This unregulated industry sold surveillance systems principally to law enforcement and intelligence agencies, products that used many of the same techniques that companies rely on to monitor their networks. But many companies had no scruples about their customers; they sold far and wide to regimes implicated in gross abuses of human rights like Sudan and the United Arab Emirates.³

The issue raised questions about the appropriate policy tools for regulating this new category of cyber technologies. It was no surprise that many of the governments using these tools did not respect human rights. But the involvement of Western companies drew attention to the role of the private sector in enabling human rights abuses. Activists and NGOs, many of which argued for limits on domestic surveillance powers, campaigned for strict regulation of exports of these technologies.⁴ In a long and arduous process, these groups successfully convinced governments to add to certain types of cyber-surveillance tools to an international list of controlled technologies, the Wassenaar Arrangement. These rules required companies to apply for export licenses to sell the surveillance systems abroad. This effort to define the appropriate language for controlling cyber-surveillance tools has challenged regulators in both the U.S. and the EU because of its complexity. While incomplete, by 2018 policies in both the EU and U.S. have taken steps to regulate cyber-surveillance exports based on human rights concerns. This result is a novel development in international rules about cyber technologies.

The debate about rules for international cybersecurity focuses on the development of norms, or expected standards of behavior for sets of actors, to govern cyberspace. Simply put, the debate is about what is appropriate for states, businesses and other actors such as civil society to do in relation to information communications technologies (ICTs). Creating norms at the state-to-state level has proved highly contentious. In the past year, the UN group dedicated to formulating cyber norms deadlocked over disagreements between the U.S., Russia and China over the scope

---

of international law in cyberspace.⁵ And scholars have argued that ostensibly agreed-upon cyber norms are honored more in their breach than in their observance.⁶ With these failures in mind, we should consider how norms develop outside traditional diplomacy among states. How can these norms apply to commercially developed surveillance capabilities? Can we understand the regulation of cyber-surveillance tools as a case of cyber norm creation? If so, to what extent was it successful? This paper argues that the effort to impose export controls on cyber-surveillance systems was a success for civil society groups that focused on constructing a highly targeted norm against providing a specific subset of cyber-surveillance tools to regimes that would use them to enable human rights abuses.

This article discusses how civil society groups contributed to creating that norm and evaluate the resulting policy outcomes with a process-focused analysis that builds off social science literature on norms creation and adoption. This discussion includes a model for analyzing the strategies that NGOs and activists, who are known as norm entrepreneurs, used to affect norms and policies. Applying that model to a dataset of more than 90 official statements, reports from NGOs, activists, business groups and government hearing transcripts, legislative debates, policy documents and proposed laws from 2011 to early 2018 shows two distinct periods in norm construction: an initial campaign for export control regulations at Wassenaar from 2011 to late 2013 and then an effort to ensure those regulations’ implementation from 2014 to 2018. The paper discusses these periods in turn, separating the implementation section into two sections for the U.S. and the EU. The analysis finds that civil society actors who focused their attention on surveillance tools with hacking capabilities achieved the most success. It also finds that the process was successful because of regulators’ ability to correct flawed approaches, norm entrepreneurs’ decision to graft their policies onto existing regimes, the role of technical experts as norm entrepreneurs, and the redirection of export controls towards human rights concerns, which also enabled changes in regulatory structures to accommodate cyber technologies.

Broadly, these findings indicate that the norms creation process can achieve success in a bottom-up fashion for cyber technologies with civil society leading the way. They raise further questions about the potential scope for such norms. With the divides between the U.S. and EU on policy implementation and the narrow focus of the regulations, it is not certain how these strategies for success can apply to other cyber governance contexts. Nevertheless, this process analysis shows how activism and regulation are evolving to respond to cyber technologies.

---


II. Background & Analytical Framework

Cyber-Surveillance Technologies

The term ‘cyber-surveillance tools’ refers to a range of ICTs that enable surveillance. This category includes mobile telecommunications equipment, monitoring centers, lawful interception systems, biometrics, digital forensics, deep packet inspection (DPI) systems, and intrusion software. Mobile telecom interception systems include International Mobile Subscriber Identity (IMSI) Catchers, devices that allow logging of nearby mobile phones and interception of their traffic. Monitoring centers and lawful interception systems allow law enforcement agencies to sweep up sources of data and collect them in order to perform analysis. For lawful intercept, governments often require by law that telecommunications companies provide law enforcement access to different forms of data collected by their systems, such as metadata, content data or location data. In this category, DPI systems enable the examination of data content in communications networks. Biometrics scan individuals’ biological or behavioral characteristics for either identification or authentication purposes, using algorithms to match scanned individuals to identities in large databases.

Finally, intrusion software tools enable remote access to a specific target through the exploitation of a software vulnerability. They use a variety of techniques, including Remote Administration Tools (RATs) and zero-day exploits, highly effective hacking techniques that make use of never-before noticed vulnerabilities. A RAT allows remote surveillance of a target through key logging, remote desktop viewing, webcam spying, audio eavesdropping, and data exfiltration.

The uses for these tools vary. Many businesses employ certain types of surveillance technologies to watch over their networks – for instance, many Internet Service Providers (ISPs) rely on DPI to detect malicious traffic and even for content monitoring for advertising. Other tools enable much more comprehensive, powerful surveillance and are only sold to law enforcement. Many police agencies use IMSI catchers to conduct sweeping surveillance of local mobile traffic. But

9 SIPRI and Ecorys, 2015 “EU dual-use export control policy review,” 172.
10 Ibid., 182.
12 Ibid. 193.
these capabilities have also spread to law enforcement and intelligence agencies around the world. Companies, notably Gamma Group in the UK/Germany and Hacking Team in Italy, have sold surveillance systems to repressive regimes, and those systems have facilitated human rights abuses in dozens of countries. Hacking Team’s Remote Control System (RCS) and Gamma’s FinFisher systems are types of intrusion software, particularly powerful because they deliver surveillance and interfaces that enable untrained users to efficiently spy on many targets at once.

In various states across the Middle East, cyber-surveillance systems enabled security forces to persecute, track, detain, and torture opponents. A report by the Citizen Lab, a Canadian security research center, found that Gamma’s FinFisher had servers in 32 countries, suggesting that it had users that included Egypt, Turkey, Turkmenistan, Venezuela, and Ethiopia. Gamma’s systems targeted independent journalists in Ethiopia and even one Ethiopian living in the United States. Nokia Siemens systems enabled Bahraini police to track and interrogate dissidents. These tools helped Bahrain find and torture democracy activists in the aftermath of the 2011 Arab Spring. Intrusive cyber-surveillance tools spread to authoritarian regimes with no constraints on their surveillance powers. Nothing stopped companies from exporting extremely powerful hacking capabilities globally. In response, NGOs argued that new rules should govern their proliferation.

**Cyber Norms — A Futile Exercise?**

Determining what is acceptable for states to do in cyberspace requires defining norms to secure and govern this new domain. The United States’ International Strategy for Cyberspace made “norms of responsible behavior” a key goal for U.S. diplomatic engagement on cyber issues. These new standards would help resolve questions like how international law applies in cyberspace and how the private sector interacts with states on cyber issues. Development of norms is taking place along multiple lines at once — from bilateral agreements like the 2015 U.S.-China accord on economic cyber-espionage to proposals from Microsoft for a ‘Digital Geneva Convention.’ But the most prominent forum for the creation of norms has been the United Nations’ Governmental Group of Experts (GGE) process, a dialogue of legal experts from 25 key states about the scope of international law in cyberspace. In 2013, the GGE came to the landmark conclusion that international law, and particularly the UN Charter, is applicable in

---


cyberspace. The 2015 GGE added that states should follow a series of norms the U.S. proposed about protecting critical infrastructure and principles of international law in cyberspace. But the 2017 GGE ended in deadlock, with the experts unable to reach consensus on a final report.

If international institutions such as the UN fail to agree on norms for cyberspace, is there hope for alternative pathways for cyber norm development? Can we even be confident that states will abide any new norms? One line of argument says that states act without regard to many of the norms that ostensibly regulate their behavior. In 2016, an unknown attacker targeted the SWIFT financial system to steal $81 million from the central bank of Bangladesh. Investigation pointed to North Korea’s Lazarus hacking group as the culprit. North Korea’s targeting of the SWIFT system violated an important norm against nation state exploitation of the financial system for monetary or strategic gain. Those skeptical of the power of norms in cyberspace point to this incident as evidence that norms fail to constrain state behavior. Another argument points to incidents such as the Bangladesh bank heist as actually supporting the concept of cyber norms. According to this view, violations of norms draw attention to the norm itself, and violations are often the only time the international community takes note of norms. The 2016 bank heist also violated numerous criminal laws, implemented over time to enforce a norm against cyber financial theft. As cyber incidents become more frequent and consequential, norms will play a greater part in how states react.

A small but growing body of literature on cyber norms has argued that norm development is occurring at a much greater number of international forums and processes than just at the UN. Efforts such as NATO’s Tallinn Manual for applying the law of armed conflict to cyberspace and the Council of Europe’s Budapest Convention for cybercrime show that states are engaging in successful norm development for cyber-related issues. Most importantly, this literature highlights the processes by which norms develop in cyberspace. Recent scholarship from Finnemore and Hollis applies social science literature on norm development to cyber norms,

arguing that analysis of how cyber norms are created is sorely underdeveloped. Their work sets
the stage for more in-depth analyses on this process. In particular, the norm development
literature can address questions like how norms change over time, how norms are implemented,
and why some norms succeed where others fail.

This conversation continues to be a major topic for debate. But one understudied area of cyber
norms relates to norms about specific cyber tools — such as cyber-surveillance systems.
Although this issue is not related to international diplomacy or the use of force in cyberspace, it
involves many of the same complexities: defining new concepts to understand ICTs and figuring
out how existing laws and policies should apply to the new domain, for instance.

Norms in Social Science Literature

Social scientists define a norm as “collective expectations for the proper behavior of actors with
a given identity.” More precisely, norms have four key elements, first, identity: the group or
individuals to which the norm applies, whether that be states, corporations, or individuals.
Second, norms regulate behavior, the specific actions that the relevant actor must take to uphold
the norm. Norms vary in the level of obligations they impose on members and whether they do
that through non-binding political commitments or sometimes through precisely defined
treaties. Third, norms have propriety, a basis for determining whether an action is appropriate
or inappropriate through mechanisms like organizational cultures, political commitments, or
laws. The basis of a norm’s propriety shapes how actors see how they “ought” to follow the
norm. Fourth, norms involve collective expectations, that is, shared constructions among actors
about what following them means in relation to each other. These elements make norms highly
dynamic, constantly changing in response to actors’ interpretations and practices relating to the
norm. Scholars have underlined that norms are nearly always in flux as they adapt to varying contexts.

Norms may spontaneously form, but motivated actors may also promote them. Scholars such as
Cass Sunstein have highlighted the role of norm entrepreneurs—actors interested in altering
political norms—in agitating for changes in collective expectations. These can be activists,
non-governmental organizations (NGOs), companies, international organizations or even states,
any actors that attempt to change how other influential actors approach the issue at hand. Among
these, civil society groups are some of the most active norm entrepreneurs. The term civil society
refers to the constellations of NGOs, community-organizations, social movements, labor unions,

---

32 Finnemore and Hollis, “Norms for Global Cybersecurity,” 443.
and other groups that make up the “third sector” of society outside government and business. While civil society is often associated with well-known international NGOs like Amnesty International and Oxfam, I define it broadly, to mean any actor not part of or affiliated with a government or business. The most notable case of civil society norm entrepreneurship was the international campaign to ban landmines. This campaign is a classic example of the power of transnational network advocacy to bring about a powerful norm against deploying a long-existing tool of war.

It makes sense to think of the work of norm entrepreneurs in stages, as defined by Finnemore and Sikkink’s framework for the evolution of political norms. First, norm entrepreneurs put forth the proposed norm in the “emergence” phase, second, the norm achieves widespread acceptance in what is termed a “norm cascade,” and third, states and people internalize the norm. In the emergence stage, norm entrepreneurs use persuasion to promote their proposed norm to influence the state and the private sector. Proponents that oppose the creation of a new norm often contest norm entrepreneurs’ efforts in this stage. As a norm gains acceptance, states begin to promote it themselves. Once a large enough amount of states adopt a norm, socialization pressures begin to apply to reticent states, passing a “tipping point” that leads to a cascade of norm acceptance. This upward path is not certain for every proposed norm. In fact, many norms fail, sometimes because of a lack of acceptance among key actors or because of a decision by norm entrepreneurs themselves not to pursue the norm.

In this struggle to change attitudes and rules, norm entrepreneurs have three different methods for developing norms: incentives, socialization, and persuasion. The first tactic, incentives, is most available to powerful actors like states that can use coercive measures like laws or positive rewards like trading partnerships to achieve their preferred norms. Ultimately the goal of these tactics is internalization, achieving such widespread acceptance of the norm that actors comply without any incentives. Socialization is one of the most effective ways of achieving that goal, as it involves the process by which new members are inducted into standards of behavior. In other words, it is becoming part of the club of actors that do things in a certain way. To do this, norm

---


entrepreneurs might pressure states to conform to certain standards because, for instance, “this is how all developed economies manage it.” But the most common way that norm entrepreneurs, particularly civil society groups like activists and NGOs, promote norms is through persuasion. This method is all about exchanging information that is designed to change opinions and attitudes about a particular issue.\(^{42}\)

Norm entrepreneurs use these tools as elements of broader strategies for promoting norms, ultimately seeking to reshape how society approaches an issue by altering perceptions, rules and behaviors. Finnemore and Hollis call this process “strategic social construction,” describing it as a series of choices by which norm entrepreneurs attempt to cultivate new norms. A key way that entrepreneurs persuade audiences to change their attitudes is through **framing**. Actors frame an issue when they “use language that names, interprets, and dramatizes the problem—and on that basis propose a norm to address it.”\(^{43}\) More formally, Benford and Snow define a frame as “action-oriented sets of beliefs and meanings that inspire and legitimate” norm entrepreneurs’ activities.\(^{44}\) Frames become more effective when norm entrepreneurs form and align with organizational platforms, venues for promoting their proposed norms through newly-created or pre-existing groups or institutions.\(^{45}\) For example, the creation of the Vienna Protocol for the Protection of the Ozone Layer was a key vehicle for environmentalists to promote norms to regulate CFCs emissions.\(^{46}\)

**Grafting** onto existing organizations to enact change can be equally effective, as that process takes advantage of the fact that the platforms already exist and could have legitimacy among key actors.\(^{47}\) Finally, norm entrepreneurs use **linking** to connect their arguments to broader subjects to increase their legitimacy and make their cases more compelling.\(^{48}\) This practice allows norm entrepreneurs to make use of more general issues of concern like great power competition or upholding treaty obligations to argue for their specific norms. And, as norms progress from emerging to being implemented, these strategies change with the context, altering to fit the stages of the process. For instance, framing is crucial when a norm is proposed, but the organizational platform where that norm is proposed matters more for the implementation phase. Visualizations of these techniques are available below in Figure 1.

---

\(^{42}\) Finnemore and Hollis, “Norms for Global Cybersecurity,” 450.

\(^{43}\) Ibid., 447.


Finnemore and Hollis emphasize that they cannot predict which combinations of these tools and choices about norm promotion will lead to successful norm creation. But they do provide a useful means of assessing the norms process by looking at the trade-offs that entrepreneurs make in the content, targets, context, linkages, organizational platforms, and level of desired commitment to their proposed norms. Given the complexity of cybersecurity problems and existing international affairs dynamics, recommending one particular approach to cyber norms is bound to fall short. But the social science literature on norms provides a framework for retrospective analysis and comparison across cases of norm development. It gives ways of discussing the strength of various norms and the means to understand the norms development process, that is, how that state of affairs evolved over time.

Existing literature leaves unresolved key questions about how these trade-offs and tools affect each stage of the norms development process. In particular, cyber technologies like hacking tools, with their complexity and constant evolution may pose challenges for traditional norm entrepreneurs in terms of framing and finding the regulatory institutions to implement their desired norms. Analyzing cyber norms through the norms development framework reveals answers about how cyber norms evolve and how cyber technologies affect the practices of norm entrepreneurs.

---

49 Finnemore and Hollis, “Norms for Global Cybersecurity,” 462.
50 Ibid., 463 – 473.
A Framework for Norms Regulating Surveillance Exports: Methods of Analysis

Civil society groups used every one of these techniques to build a norm against exports of cyber-surveillance tools to human rights violators. This article analyzes how each norm entrepreneur used framing, linking, and organizational platforms and discuss how their targets, audiences, context and level of desired internalization of their proposed norm affected the debate about cyber-surveillance technologies. Furthermore, the article discusses to what extent each of norm entrepreneurs realized their stated goals, connecting the policy outcomes with the choices and trade-offs they made. A qualitative review of over 90 official statements, reports, laws and regulations, and public comments from both the U.S. and the European Union leads to a cross-comparison of the norms development processes between the two jurisdictions. This data provided a range of viewpoints from influential norm entrepreneurs and their audiences within and outside government.

Ultimately, the analysis of the norms development process for surveillance technologies illustrates both the successes of civil society and their limits. It is a story of passionate, technically savvy individuals who were motivated to work for the common good and of governments making strategic calculations about powerful hacking capabilities. Understanding that story though the lens of norms reshapes our conception of why export controls for cyber-surveillance matter. It points to the role of civil society in shaping cyber governance and underscores the fact that even for complex, rapidly evolving technologies, the process of building new standards of behavior is fundamentally social — between and among people — and will continue regardless of the status of the UN GGE or the Budapest Convention or any other international accord.
III. Emergence of Proposed Surveillance Norms, 2011 – 2013

As with any developing norm, the first stages of public attention and initial framing of the issue was crucial. These starting steps were about defining the terms of public debate and about determining which policy instruments might even be able to regulate the cyber-surveillance trade, given its novelty. In this process, the critical norm entrepreneurs came from disparate corners of civil society — from Canadian universities and London-based NGOs to activists in Bahrain. Out of the mix of stories about authoritarian repression and the proliferation of powerful hacking tools emerged three distinct framings of the problem: 1) surveillance as an Internet freedom issue, 2) human rights abuses as failures of corporate due diligence and 3) surveillance tools as “digital weapons.” Each of these led to policy outcomes, varying in their levels of success in regulating surveillance exports and in building a cohesive norm. This section details those frames and their policy outcomes and analyzes those outcomes in terms of their contributions to defining a norm for cyber-surveillance exports.

Civil Society Groups: Old and New Players

Surveillance as an issue cut across divides between “traditional” NGOs like Amnesty International and newer groups that focused on technological impacts like Privacy International. A new and very prominent group outside the NGO community was the Citizen Lab, a Toronto-based research group that contributed much of the software analysis that documented specific Western-developed surveillance systems during the Arab Spring. This research then linked with advocacy from human rights-focused NGOs such as Amnesty International, Human Rights Watch, Bahrain Watch, and the International Federation for Human Rights (FIDH). These groups focused on what surveillance software enabled authoritarian regimes to do, including arbitrary detention of dissidents and journalists, tracking political opponents abroad, and even torture. NGOs that promoted privacy and Internet freedom also drew heavily on the Citizen Lab’s work, banding together with the human rights-focused groups. The Electronic Frontier Foundation (EFF), a U.S.-based nonprofit that describes its mission as “defending civil liberties in the digital world,” aligned with Privacy International, a UK charity that “challenges overreaching state and corporate surveillance,” to draw attention to Western companies’ role in surveillance by authoritarian regimes. Joining the NGOs, Marietje Schaake, a member of the European Parliament and liberal Dutch politician, took up the issue of surveillance exports as

---


53 Electronic Frontier Foundation, “About EFF,” [https://www.eff.org/about](https://www.eff.org/about)


part of her broader interest in digital governance and human rights.\textsuperscript{54} This loose set of groups and people sought to curb the cyber-surveillance trade for human rights reasons.

Table 1. Key Norm Entrepreneurs in the Emergence of Cyber-Surveillance Exports Norms.

<table>
<thead>
<tr>
<th>Norm Entrepreneur</th>
<th>Type</th>
<th>Focus</th>
<th>Policy Priorities</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Citizen Lab</td>
<td>Research Group</td>
<td>Internet censorship</td>
<td>Corporate accountability</td>
<td>Canada</td>
</tr>
<tr>
<td>Reporters without Borders</td>
<td>NGO</td>
<td>Press freedom</td>
<td>Export controls</td>
<td>France</td>
</tr>
<tr>
<td>Bahrain Watch</td>
<td>NGO</td>
<td>Human rights, Bahrain</td>
<td>Corporate accountability</td>
<td>UK</td>
</tr>
<tr>
<td>Amnesty International</td>
<td>NGO</td>
<td>Human rights</td>
<td>Export controls, corporate accountability</td>
<td>UK</td>
</tr>
<tr>
<td>EIDH</td>
<td>NGO</td>
<td>Human rights</td>
<td>Corporate accountability</td>
<td>France</td>
</tr>
<tr>
<td>ECCHR</td>
<td>NGO</td>
<td>Human rights</td>
<td>Corporate accountability</td>
<td>Germany</td>
</tr>
<tr>
<td>Marietje Schaake</td>
<td>Legislator</td>
<td>Digital rights</td>
<td>Export controls</td>
<td>Netherlands</td>
</tr>
<tr>
<td>Access Now</td>
<td>NOO</td>
<td>Digital rights</td>
<td>Export controls</td>
<td>US</td>
</tr>
<tr>
<td>Chris Smith</td>
<td>Legislator</td>
<td>Online civil liberties</td>
<td>Sanctions, export controls</td>
<td>US</td>
</tr>
<tr>
<td>Centre for Democracy and Technology</td>
<td>NGO</td>
<td>Online civil liberties</td>
<td>Export controls, corporate accountability</td>
<td>US</td>
</tr>
<tr>
<td>Electronic Frontier Foundation</td>
<td>NOO</td>
<td>Online civil liberties</td>
<td>Corporate accountability</td>
<td>US</td>
</tr>
<tr>
<td>Privacy International</td>
<td>NOO</td>
<td>Online privacy</td>
<td>Export controls, corporate accountability</td>
<td>UK</td>
</tr>
</tbody>
</table>

\textit{Frame 1: Surveillance tools as detrimental to Internet freedom, 2011-2012}

The research that initially brought many Western-developed surveillance systems to light connected surveillance to censorship and Internet freedom. Technical documentation from the Citizen Lab played the crucial role in linking Western companies to specific human rights abuses and to censorship.\textsuperscript{55} Its reports about Hacking Team’s RCS in the UAE and Blue Coat’s system in Syria gave groups like Reporters Without Borders (RSF) evidence to support their argument that surveillance enabled “cyber-censorship” by these so-called “Enemies of the Internet,” which included specialized companies such as Amesys and Blue Coat.\textsuperscript{56} These companies did sell traffic monitoring equipment like DPI systems that enabled Internet censorship. But Amesys and others also sold hacking systems like Amesys’ ‘Eagle’ software. The Libyan government used the Eagle system to target journalists, arresting and torturing some of them.\textsuperscript{57} In this way, RSF and other groups connected the firms that enabled surveillance, the tracking of individuals, with censorship, the control of Internet content. Since opposing censorship was at the heart of many


\textsuperscript{57} Paul Sonne and Margaret Coker, “Firms Aided Libyan Spies,” \textit{The Wall Street Journal}, August 30, 2011. \url{https://www.wsj.com/articles/SB10001424053111904199404576538721260166388}

ideas about Internet freedom, this juxtaposition framed surveillance systems as another facet of threats to Internet freedom.

This linkage leveraged Western commitments to Internet freedom to put pressure on governments to control the companies enabling surveillance. Hillary Clinton, the then-U.S. secretary of state, had made Internet freedom a U.S. policy priority in a speech in 2010. She drew attention to the role of companies that facilitate censorship at a conference in late 2011, showing U.S. policy interest in the surveillance issue. Similarly, the European Parliament embraced Internet freedom as one of its foreign policy objectives in a 2012 report penned by Marietje Schaake. This report specifically condemned EU-made technologies that enabled surveillance by repressive regimes.

This focus on Internet freedom led to action. In early 2012, the EU and U.S. enacted targeted sanctions on Syria and Iran that included any individuals or companies that sold items that as the U.S. said were, “likely to be used to facilitate computer or network disruption, monitoring, or tracking that could assist in or enable serious human rights abuses.” The EU sanctions measures said they prohibited technologies that might be “used for internal repression.” These restrictions targeted Iran and Syria, two states hostile to Western interests, barring transactions between Western surveillance companies and their governments. In one instance, these sanctions led the U.S. Bureau of Industry and Security, which administers U.S. export controls, to investigate and then reach a $2.8 million settlement with a company that unlawfully diverted Blue Coat surveillance systems to Syria. Despite their limited reach, the sanctions on Syria and Iran proved to be one of the most effective checks on surveillance exports to those countries.

As a strategy, the Internet freedom framing created demonstrable policy results but did not lead to broader regulation of surveillance exports. Rep. Chris Smith introduced a bill in the U.S.

---

66 In particular, U.S. sanctions on Iran prevent the transfer of a vast slew of ICTs, so much that some have even argued the sanctions are detrimental to pro-democracy activists who need secure communication platforms. See Peter Harrell and Collin Anderson, “U.S. Sanctions Abet Iranian Internet Censorship,” Foreign Policy, January 22, 2018. http://foreignpolicy.com/2018/01/22/u-s-sanction-abet-iranian-internet-censorship/#
Congress in 2013 that would have mandated the U.S. develop a global Internet freedom policy and that would have enacted export controls on telecommunications surveillance and censorship systems.\textsuperscript{64} It did not get to the House floor, possibly because of earlier opposition from tech companies.\textsuperscript{65} In terms of building a norm, the U.S. and the EU did not enact any policies that curbed surveillance exports to friendly regimes like the UAE and Bahrain. This frame’s overall impact on norm development is ambiguous; it instead receded as norm entrepreneurs made clearer distinctions between systems used for censorship and targeted surveillance technologies.

Frame 2: Corporate Social Responsibility for Human Rights Violations, 2012-2013

To civil society, cyber-surveillance was an issue about establishing the responsibility of businesses themselves as well as governments to curb exports that could potentially harm human rights. This view was a core viewpoint for many human rights groups who strongly supported the concept of enforcing corporate social responsibility. They saw the clear linkages between Western-developed systems and specific human rights violations as an opportunity to establish companies’ liability. For instance, Privacy International filed complaints with the National Contact Points for the Organization for Economic Cooperation and Development (OECD) in the United Kingdom and Germany, alleging that certain surveillance exports violated the OECD’s Guidelines for Multinational Enterprises.\textsuperscript{66} The guidelines, which are non-binding, have numerous provisions related to the obligations of enterprises on the human rights impacts of their products. Complaints can be filed to arbitration by the NCPs. Privacy International’s approach sought to build a norm through precedent by specifically showing that surveillance sales violated human rights protections.

This frame cast human rights abuses as failures of corporate responsibility. Privacy International accused Gamma and Trovicor of neglecting to assess the human rights impacts of their products as much as it accused them of actual complicity in enabling surveillance and torture.\textsuperscript{67} But compliance with the complaint system is purely voluntary. Privacy International knew this, of course. The complaint aimed to persuade companies to voluntarily adopt due diligence standards themselves to avoid future public complaint actions.\textsuperscript{68} Interestingly, by framing the issue as a failure of corporate responsibility, Privacy International proposed a norm that did not focus on any particular technology like intrusion software or network monitoring equipment.

The corporate social responsibility frame allowed NGOs to take direct action by filing legal complaints against companies. But actually building a norm requires showing the downsides of non-compliance. Imposing costs proved difficult. Germany’s NCP threw out the complaint against Trovicor, saying there was not enough direct evidence linking its products to Bahrain’s

\textsuperscript{64} H.R. 491 “Global Online Freedom Act of 2013,” 113\textsuperscript{th} Congress. https://www.congress.gov/bill/113th-congress/house-bill/491
government. The UK NCP eventually ruled that Gamma had violated the Guidelines by not pursuing due diligence but said there was not enough evidence to prove it had facilitated human rights abuses. A judicial inquiry against Amesys in France for its role in providing surveillance systems to Libya has languished in appeals. For a variety of reasons, no court or other judicial body penalized any company for its role in exporting surveillance. Absent costs imposed by the courts, the norm for corporate due diligence in the surveillance sector was weak.

Frame 3: Surveillance exports as dual-use digital weapons, 2012-2014

The last and most significant way that civil society groups described surveillance tools was calling them “digital weapons.” It affected the debate in several different ways. First, it created a linkage with the arms trade. MEP Schaake made that connection explicit, saying “these technologies can be effective as weapons,” and calling for “stopping the digital arms trade.” States control arms exports for many reasons, including economic, security, and diplomatic rationales, and usually not humanitarian interests. These security interests are powerful reasons for regulating trade. The digital weapons frame casted surveillance tools as directly able to inflict harms and attracted attention from policymakers interested in cybersecurity.

Second, the digital weapons frame closely linked the surveillance tools issue to the broader topic of controls on vulnerabilities and “cyber weapons.” In the aftermath of the discovery that the Stuxnet virus had used four different zero-day vulnerabilities, the trade in software exploits had emerged as a potential cybersecurity threat. The U.S. Congress also focused its attention on the issue, including requirements in the annual U.S. defense authorization bill for 2014 for the president to create a policy to control “the proliferation of cyber weapons.” This term, “cyber weapons,” often refers to software programs that use exploits, including zero-day vulnerabilities to deliver payloads of malware to a specific target. Regulating cyber weapons would mean controlling cyber-surveillance tools as well as regulating firms involved in trade of exploits

---

themselves. Schaeke made this connection explicit in a speech before the European Parliament, advancing arguments for controlling hacking tools for both security and human rights reasons.

This frame also implicitly excluded software systems that enable mass Internet traffic monitoring, such as Blue Coat’s network surveillance systems.

Casting surveillance software as digital weapons influenced how states chose to regulate their exports. In particular, as norm entrepreneurs framed surveillance tools as dual-use digital weapons, attention focused on export controls as the policy tool for regulating cyber-surveillance items. Export controls are requirements that companies that want to sell a product abroad get approval through a licensing process. They are not prohibitions on exports but rather a duty to get governmental approval for international technology transfers. Companies apply for an export license for a given product and destination country. This process usually involves sharing a significant amount of information about the item, the end-user, the destination country, and the company itself.

To coordinate export controls, groups of countries agree on lists of items they wish to control, thereby controlling exports on a global level. The Wassenaar Arrangement is one such agreement, a 41-member state international framework for coordinating export controls on dual-use technologies. Founded in 1996, it grew out a Cold War-era organization that sought to limit exports of dual-use technologies to the Soviet bloc. After the Cold War ended, Western countries expanded the “club” of industrially-advanced countries to include Russia and South Africa. The Wassenaar Arrangement focuses on technologies with defense implications, especially technologies related to proliferation purposes. Its members meet annually to decide on revisions to its control lists.

There were potential alternative types of export controls that could have applied to surveillance items. The U.S. imposes export controls on items for crime control and crime detection, including handcuffs, stun guns, and instruments designed for torture. The U.S. specifically says these controls are intended to promote human rights. The EU strictly regulates the trade in goods that could be used for capital punishment or torture, including prohibiting the export of lethal injection drugs to countries with the death penalty. Marietje Schaeke equated surveillance tools with items for torture in her report on the EU’s digital freedom strategy, saying they should be categorized as “single-use.” But neither the U.S. crime controls nor EU anti-torture regulations cover the other jurisdiction. For civil society groups who hoped for a control that would apply for the entire surveillance industry, achieving regulatory change required framing surveillance as “dual-use” rather than “single-use” and required focusing on their security implications.

---

Civil society framed digital weapons as “dual-use” less through language through a series of strategic decisions. Most importantly, Privacy International filed a complaint with UK authorities, accusing the UK government of failing to impose export controls on Gamma’s FinSpy system. Privacy International argued that the associated human rights concerns with FinSpy’s use mandated that Gamma obtain an export license. The UK’s response was that the government had indeed required Gamma to apply for a license — because its products involved controlled cryptographic systems, not because of their human rights implications. These controls came from the Wassenaar list. In its response about the human rights concerns, the UK disclosed that “such issues are currently being ventilated amongst the parties to the Wassenaar Arrangement at the initiative of the United Kingdom.” It is notable that it was the British and French governments that took up cyber-surveillance at Wassenaar, there were high profile cases of surveillance exports from both states that were linked to human rights abuses in the Middle East (Gamma for the UK and Amesys for France). There is not publicly available information as to why other governments with significant surveillance industries like Germany did not make proposals. In the EU, Schake specifically pushed for discussion of surveillance technologies during the review of the EU’s dual-use framework, arguing for controlling it based on “shifting EU foreign policy objectives.” These actions focused the policy forum for regulating digital weapons to export control frameworks and in particular on the Wassenaar Arrangement.

British and French efforts at Wassenaar led to results. The Wassenaar members agreed to include two specific types of technologies, IP network surveillance systems and intrusion software, in the Wassenaar Arrangement’s dual-use list. This result did not show a human rights-based norm for surveillance exports. In fact, the official statement from Wassenaar was that the control was because these technologies, “under certain circumstances, may be detrimental to international and regional stability and security.” Even the UK’s BIS indicated it was concerned about the systems’ potential for “espionage,” not their connection to human rights abuses.

---

84 Ibid.
88 Jones, “Cyber war technology to be controlled,”
Table 2. Frames, Targets, Issue Linking and Policy Outcomes in the Emergence Phase

<table>
<thead>
<tr>
<th>Frame</th>
<th>Norm Entrepreneurs</th>
<th>Target Audiences</th>
<th>Standard of Behavior</th>
<th>Linked Issues</th>
<th>Policy Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Harming Internet Freedom</td>
<td>Amnesty Int. RSF</td>
<td>U.S. government</td>
<td>Governments should pressure other states not to use surveillance to repress internet freedom</td>
<td>Democracy promotion</td>
<td>2012 U.S. and EU sanctions on Iran and Syria</td>
</tr>
<tr>
<td></td>
<td>Citizen Lab Chris Smith</td>
<td>UK government Pro-democracy</td>
<td>groups</td>
<td>Freedom of expression</td>
<td></td>
</tr>
<tr>
<td>Corporate due diligence failure</td>
<td>Privacy Int. EFF FIDH RSF</td>
<td>OECD Courts Human rights activists</td>
<td>Companies should be held responsible for human rights abuses enabled by their products</td>
<td>Corporate social responsibility Human rights due diligence</td>
<td>2014 UK OECD Judgment against Gamma</td>
</tr>
<tr>
<td>Dual-use digital weapons</td>
<td>Privacy Int. RSF Marietje Schaake</td>
<td>U.S. government EU governments</td>
<td>States should prevent companies from exporting cyber-surveillance to human rights violators</td>
<td>Cyber arms control Vulnerabilities trade</td>
<td>2013 Wassenaar export controls additions</td>
</tr>
</tbody>
</table>

Wassenaar as Cyber-Surveillance Regulation Without Norms

In December 2013, it appeared that the efforts of civil society, the privacy NGOs and human rights groups had paid off. Governments had agreed to regulate cyber-surveillance exports, albeit with an unusual policy tool. Dual-use export controls are not based on human rights concerns. Yet strategic choices and the digital weapons frame ultimately led to the Wassenaar Arrangement as the platform for civil society’s proposed norm. As detailed in Table 2 above, only the digital weapons frame led to comprehensive regulation of cyber-surveillance tools. At the same time, states had other interests in controlling cyber-surveillance tools, particularly related to regulating the vulnerabilities trade. Export controls were not an ideal choice for human rights-focused civil society groups to use to regulate cyber-surveillance tools but they were the best strategic choice. The strategy succeeded in implementing regulations on cyber-surveillance tools but it was not clear whether these would apply for human rights reasons. The “digital weapons” frame instead highlighted the potential for export controls to regulate new sets of cyber technologies like surveillance tools. But civil society could not be confident that states would actually implement the export controls to reflect a norm against proliferating cyber-surveillance tools to human rights violators. Wassenaar was only the first stage in a complex process of implementing a global norm for cyber-surveillance items.
IV: Export Controls and U.S. Cybersecurity Norms, 2014 – 2017

In the United States, implementing the Wassenaar controls led to a sharp reaction from cybersecurity researchers and businesses involved in the offensive cybersecurity industry. The debate shifted because of two factors: first, input from elements that constituted a civil society for the cybersecurity industry such as academic and independent researchers, and second, the U.S. government’s approach to implementing the controls as regulations. This debate focused on the purpose of the intrusion software controls, as it was not clear whether the U.S. government intended the controls to regulate the vulnerabilities trade or to prevent repressive regimes from receiving surveillance tools. Private industry argued that export controls were a bad policy tool to implement a norm against the export of cyber-surveillance tools to repressive regimes. Partly, this norm clashed with a strong cybersecurity-focused set of actors, particularly among policymakers in the U.S. Congress. This section discusses how this group of actors reversed U.S. policy and effected certain corrections to the policy implementation of the controls. Ultimately, the U.S. did not reject the norm but refrained from implementing it because of objections from the cybersecurity community.

“Offensive” Technology and the Wassenaar Controls

A key issue for the U.S. implementation process was about the particular approach that Wassenaar took to define intrusion software. The Wassenaar controls did not limit intrusion software to surveillance tools. The basic definition was any software system that evaded monitoring or protective systems to either extract data from a computer system or to modify the “standard execution path” of a program to allow external control.\(^89\) It included any software that fit these parameters, regardless of whether it was offensive or defensive in purpose. Another complication was that Wassenaar did not impose the export controls on intrusion software itself. Instead, it put the license requirements on software systems that operate intrusion software and on technology for the “development” of intrusion software.\(^90\) In a sense, this approach reflected some of the ambiguity inherent in attempting to regulate ‘digital weapons’ — a term that is not well defined itself. But these complexities created significant confusion about the scope of the Wassenaar controls. Some such as Access Now’s Collin Anderson contended that the controls applied narrowly while others warned that they could apply to a wide range of software security tools used primarily for legitimate defensive purposes.\(^91\)

Individual member states in Wassenaar are responsible for actually implementing the controls. The U.S. government took a notably long time for the interagency process to come to a consensus on how to implement the controls — three times as long as it usually takes. Then it


\(^{90}\) Ibid., 73.


issued a proposed rule open to public comments, a first on Wassenaar controls. That interagency process would have run through a committee chaired by the Commerce Department that included the Departments of State, Energy, and Defense. Within the Department of Defense, the relevant agency for export control licensing is the Defense Technology Security Administration (DTSA), but another potential player is the National Security Agency (NSA). NSA, as the agency primarily involved both purchasing vulnerabilities and using them for cyber intelligence operations, has a significant interest in regulations for the vulnerabilities market. Given this context, the proposed rule from Commerce has several additions that support the hypothesis that the U.S. government intended the controls to cover offensive cyber technologies, not just surveillance tools.

First, the Commerce rule put the controls into the informal category of “cybersecurity” rather than surveillance, emphasizing their relation to hacking. Second, it expanded the scope of its controls by saying that they applied to penetration testing tools and to propriety research into vulnerabilities. In contrast, guidance from the United Kingdom on implementing its controls on intrusion software said that most penetration testing would be exempt from license requirements because of a mass-market software exemption. Commerce removed the mass-market exemption for intrusion software. Third, in its discussion of licensing policies, Commerce said that it would presumptively deny products using rootkit or “zero-day exploit capabilities.”

In a subsequent FAQ, this focus on “offensive” technologies showed more clearly. The FAQ explicitly placed intrusion software in the larger category of “malware” in one answer and justified the specific focus on zero-days and rootkit functionality because they are “features more likely to be found in offensive systems or products.” From these statements, it is clear that Commerce viewed the controls as essentially regulating offensive cybersecurity tools and that Commerce tailored its regulations to that end.

The government’s interpretation influenced the reactions from the cybersecurity industry. Commenters on the BIS rule such as Rapid7, a firm that produces the vulnerability testing tool Metasploit, emphasized that defensive security products often deploy offensive techniques to test

---

Similarly, comments from the CERT underlined the lack of a distinction between defensive and offensive security tools, arguing this factor posed a problem for Commerce’s intent to regulate “attack” tools. This disagreement was at the core of the security industry’s and security researchers’ objections to the controls. From a wider perspective, the debate shifted entirely from export controls as way to advance human rights impacts to export controls as means for controlling offensive cyber tools. The same export controls could not accomplish these vastly different goals.

The Security Research Community as a Counterpoint to Norm Entrepreneurs: Framing Export Controls as Ineffective for Cyber Technologies

The proposed rule galvanized strong opposition from software security researchers and entrepreneurs. As the debate moved from the international level to the domestic implementation of Wassenaar, the security research community re-centered the terms of discussion to the unintended consequences of export controls. In doing so, they marked their own emergence as actors that countered civil society’s framing of surveillance regulation. They drew legitimacy from their technical knowledge and experience, using that credibility to influence policymakers who wanted to make cybersecurity a top concern.

The research community identified several key equities at stake for their work in the proposed rule. First, they characterized the reach of the controls as unfeasibly broad, arguing that the terms the Commerce Department laid out covered exchanges of vulnerability information, offensive security research techniques, and even bug bounty programs. Second, they said that the controls unfairly singled out “offensive” security research as problematic. This concern struck at the core of the “hacker” identity that many in the research community, particularly independent researchers, feared the government aimed to curtail. Dan Kaminsky, a well-known “white hat hacker,” made the case for the importance of offensive activities by saying, “A lot of people are going to have to learn how things break, if we are to have any hope of making things that survive attack.” This perspective led to far-reaching claims that the Wassenaar rules would “potentially criminalize hacking.” Such rhetoric made the export controls seem to be an existential threat to the security community – and they warned that their work was crucial to the security of all computing systems. The language about threats to offensive security research obscured the normative arguments about the use of export controls for human rights ends. It helped unite a chorus of voices from independent researchers, university centers, entrepreneurs, and researchers at large companies like Symantec and FireEye.

---


The last argument that security researchers advanced was that export controls were a fundamentally inadequate means of controlling cyber technologies. This “cyber exceptionalism” narrative was common in reactions from the cybersecurity community to regulation generally, but it also drew from researchers’ past experience with export controls on cryptography. The so-called “crypto wars,” during the 1990s about export controls on advanced cryptography formed the basis for much of researchers’ pre-existing antipathy towards export controls. Until the late 1990s, the U.S. government had placed strong encryption systems on the munitions control list. A coalition of privacy advocates, researchers and the nascent computing industry successfully campaigned for the relaxation of most export restrictions on cryptography. Researchers like Sergey Bratus made a direct analogy from the intrusion software controls to this period, linking the encryption controls to security failures and predicting the intrusion software controls would lead to the same outcome. The acrimony between the government and the research community during that period resurfaced in the intrusion software debate, leading to criticisms of export controls as an inadequate way to regulate cyber technologies.

These critiques focused on export controls’ effectiveness. Researchers pointed out that it would be easy to subvert the licensing process by sending code over the Internet. They also argued that “malicious” actors would not bother with licensing at all. Some even questioned the efficacy of export controls for controlling all modern technologies, calling it a “Cold War relic.” This framing questioned the legitimacy and effectiveness of export controls for cybersecurity. As issue framing, it was effective because of the security research community’s technical expertise. That knowledge had a great deal of credibility because of the research community’s prominent role in the security industry.

To refer to the security research community is often also to refer to the security industry. Researchers cross boundaries between academic institutions, private companies and independent freelancing, with the same individuals having multiple affiliations. Even large corporations such like Symantec respect the research community because their products rely on research to identify new vulnerabilities. The vital role of research in the cybersecurity industry allowed

researchers to claim that their work was important for cybersecurity, economic security and even national security. They interpreted the proposed rule as a threat to their continued viability.

The Influence of the Software Security Industry: Cybersecurity As a Policy Priority

American software security companies immediately perceived the Commerce proposed regulations as a threat to their business. Symantec was likely the largest company affected. It led industry response, organizing companies such as Intel, Microsoft, FireEye, Raytheon and others into the “Coalition for Responsible Cybersecurity” that lobbied the U.S. government against the rule.111 The coalition joined the Business Software Alliance (BSA), a powerful lobby for software firms that Microsoft founded in 1988 to promote anti-piracy legislation.112 To oppose the export controls, leading security industry firms had created a specialized lobbying platform (the coalition) and joined to an already-existing business group with expertise and funding.

In their comments to the Commerce rule, software firms described the regulations as harming cybersecurity. Rapid7, maker of the ‘Metasploit’ tool, said the rules would have a “chilling effect” that would prevent global cybersecurity research and undermine innovation.113 Comments from Symantec, FireEye and the BSA all cited a heavy compliance burden on their operations, saying they would have to apply for dozens, if not hundreds of complex licenses to do everyday threat sharing and research exchanges.114 This discourse emphasized the effect of the burden on firms’ ability to provide cybersecurity services and to work with cyber security researchers. It emphasized cybersecurity’s importance for national security and strategic competitiveness rather than how the regulatory burden would affect their bottom line. When industry did bring up economic matters, as did the comment from the Coalition for Responsible Cybersecurity, it focused on how negatively affecting the cybersecurity industry would harm “the development of cybersecurity defenses in the United States.”115 Firms also linked their framing to an important U.S. government cybersecurity priority: information sharing. Symantec argued that export controls, particularly “deemed exports”—transfers to foreign nationals working in the U.S.— would undermine U.S. efforts to encourage information sharing.116

Both these strategies, framing in terms of cyber defense and linking to information sharing, showed that companies aimed to appeal to U.S. government strategic priorities in cyberspace, as

116 Cheri McGuire, “Symantec Comments,”
articulated in the 2011 White House Strategy for Cyberspace, which cited information sharing and resilient networks as key for a “secure and reliable” cyberspace. But they also revealed the centrality of the private sector to U.S. cybersecurity efforts. Companies saw themselves as performing a task crucial to national security, and along similar lines to security researchers, wanted the government to support their work rather than regulate it.

While the public comments were the main pathway for both industry and researchers to campaign against the rules, there were broader efforts to push back against export control regulation. This took the form of pressure on Congress. Representatives from Symantec, Microsoft and the Information Technology Industry Council appeared before a House hearing on “Wassenaar: Cybersecurity and Export Control,” in early 2016. None of the present members or witnesses favored implementing the existing rule. Proposed policy fixes ranged issuing a revised rule with exceptions for vulnerability research activities and penetration testing products to having the State Department attempt to remove the controls from the Wassenaar list through renegotiation. Symantec and many other larger software businesses supported the second option. In this regard, their framing of the proposed rule as a threat to national security helped make the case to the State Department, which weighs national security and foreign policy concerns more heavily than economic issues.

An interesting corollary to the industry reaction is how civil society in the U.S. largely echoed researchers’ arguments. Though these groups emphasized the importance of export controls as a tool for controlling the cyber-surveillance proliferation, they also underlined that export controls were, in the words of Collin Anderson, “not a panacea” to the surveillance trade. Broadly, they recommended a revision of the proposed rule, particularly highlighting the potential for damage to the work of security researchers. The Electronic Frontier Foundation (EFF) used the opportunity to argue for the elimination of all controls on encryption, which was one of its top priorities. EFF campaigns on behalf of stronger encryption because encryption is a crucial technology to mitigate online surveillance, from all sources, including ISPs and intelligence agencies. Even though the Citizen Lab did not comment directly on the proposed rule, its founder, Ron Deibert, in testimony to a Canadian Senate committee, did note that U.S.

researchers and firms opposed it.\textsuperscript{124} What is notable about civil society contributions is their lack of disagreement with researchers and industry. All agreed that the proposed rules were bad. In this situation, that unified opposition contributed to the Commerce Department’s eventual retreat.

\textit{U.S. Policy Reversal – Cybersecurity Norms in Opposition?}

It was not a surprise that the Commerce Department reversed course and declared that it would not implement its proposed rule. Far more interesting is how the companies and groups opposing it were able to convince key policymakers to renegotiate the Wassenaar rules themselves. In this process, the January 2016 House committee hearing was critical. Congressional representatives emphasized the importance of cybersecurity and largely lauded the private sector’s role in opposing the Commerce Department’s rule.\textsuperscript{125} The subcommittees involved motivated this approach — their portfolios involve homeland security and cybersecurity, not human rights or national security. Members mentioned “human rights” only four times during a three-hour hearing, instead focusing their attention on the Commerce Department’s failures to consult technical experts. Officials from Commerce and State testified that while at negotiation they understood the intrusion software controls to be narrow in scope, on writing proposed rules, they came to understand the language covered a broad range of systems.\textsuperscript{126}

On a bipartisan basis, legislators pressed the officials about the possibility of renegotiating the intrusion software language at Wassenaar.\textsuperscript{127} Members also emphasized that it was necessary to demonstrate leadership at Wassenaar on the issue. Supplementing the excoriation State and Commerce officials received during the hearing, Reps. Langevin and McCaul sent a letter backed by 125 members of Congress to the White House expressing their opposition to the Commerce rule on national security grounds.\textsuperscript{128}

Industry opposition killed the Commerce rule. It was congressional pressure that convinced the Obama administration to commit to renegotiate Wassenaar. The Langevin-McCaul letter and the January 2016 hearing led to a response from the Secretary of Commerce that the U.S. had proposed in the 2016 Wassenaar negotiations to eliminate the controls on “technology for the development of intrusion software.”\textsuperscript{129} Congressional pressure continued into the next

\textsuperscript{126} Ibid., 66.
\textsuperscript{127} Ibid., 85.
administration as the U.S. did not achieve any changes at the 2016 meeting. After over eighteen cumulative months of renegotiations, the U.S. succeeded in achieving alterations to the Wassenaar language in December 2017.

Broadly, these changes added exemptions for items that carry out operator-authorized updates and for items associated with intrusion software that are used for vulnerability disclosure or cyber incident response activities. To negotiate the changes, the U.S. team included technical experts from the cybersecurity industry, including Katie Moussouris and Iain Mulholland, who had criticized the 2015 proposed rule. This choice shows a change in attitude to include the advice of private sector experts. Commerce and State started to welcome researchers’ input, and it is quite notable that these non-government experts were part of the U.S. delegation. As for the research exemptions, the Commerce Department has yet to decide whether it will implement the revised language or go back to Wassenaar for further renegotiation.

Figure 2. Process of Redirecting the “Digital Weapons” Frame Towards Cybersecurity, with Policy Results Shown on the Right.

---

Fitting the U.S. response into a linear process of norm development is difficult — as shown in the complex re-direction of cyber-surveillance debate displayed in Figure 2. But it would be a mistake to interpret the U.S. as rejecting the NGOs’ proposed norm. As a policy matter, the U.S. temporarily halted its implementation of the Wassenaar rules because of concerns about its effect on the cybersecurity industry. However, the U.S. did not reject the norm against cyber-surveillance proliferation. By 2018, the principal policy result was the 2017 exemptions to the intrusion software definition for vulnerability research. The U.S. still agreed on the export controls. If anything, the consequence of the backlash in the U.S. was to clarify and narrow the scope of the original 2013 controls, focusing them on cyber-surveillance tools. Whether the U.S. originally agreed to the controls for human rights reasons is unclear because it is likely the U.S. originally adopted the controls to regulate the vulnerability trade and then quickly discovered that was not a practical goal.

Differences in interpretation about the scope of the export controls motivated the industry-led backlash, not normative differences about cyber-surveillance tools. Security researchers played an essential role in providing technical expertise and evidence that persuaded both companies and policymakers to adopt an expansive view of the controls’ scope. This impact is parallel to the role the Citizen Lab played for the human rights focused norm entrepreneurs. However, security researchers were able to redefine the debate, drowning out normative discussions with their concerns about what they saw as burdensome, unnecessary regulation. And those concerns resonated with what both the Commerce Department and lawmakers in Congress valued: cybersecurity.

Policy outcomes reflect this divergent interpretation. The key policy forum was the U.S. Congress — specifically the House subcommittees focused on cybersecurity. These lawmakers had powerful domestic incentives for supporting U.S. business interests and cybersecurity as a national security priority. With the information they had, these lawmakers and industry leaders focused on the potential broad impacts of the controls on cybersecurity, not how the controls would promote human rights. Advocates concerned about privacy simply did not have the constituency or the activation of established civil society groups that could mobilize voters, like groups such as Privacy International did in Europe. And, a different breed of civil society, security researchers, played a critical role in mobilizing opposition from industry. This factor combined with the committees that possessed jurisdiction over the Commerce Department to undermine support for the cyber-surveillance norm in the United States. Without pressure from the legislative branch, the executive would not have changed course and perhaps would attempted to implement a revised rule with exceptions for research. The U.S.’s clout at Wassenaar enabled it to obtain the December 2017 revisions. Ultimately, the activation of different communities in the United States, particularly researchers, pushed U.S. policy to hold off on implementing the Wassenaar controls. This approach contrasted sharply with developments in the European Union.
Implementing the export controls in the European Union also gave rise to concerns about the effectiveness of export controls for digital technologies. The key difference between the EU and U.S. cases was relative power and influence of different civil society actors and industry groups. In the EU, the civil society groups that had the most input into the policy debate were privacy-focused human rights NGOs, not cybersecurity researchers as in the U.S. This difference led to an almost opposite result than in the United States. Because of the influence of NGOs, the EU undertook a remarkable effort to adapt export controls to cyber-surveillance tools. Human rights-focused norm entrepreneurs sought to integrate human rights into the dual-use export control framework—a novel purpose for dual-use. One way that EU policymakers proposed to do this was through applying a “human security” concept to cyber-surveillance tools. This concept could have applied human rights standards to nearly all export licenses. Ultimately, the reform effort has focused itself on cyber-surveillance tools, limiting and strengthening human rights protections mainly for these specific technologies. The dynamic between NGOs and EU policymakers is particularly interesting in that civil society groups took on an important role in shaping and directing the dual-use export control reform process. Their success in reforming EU policies shows how civil society groups can be effective at implementing their proposed norms.

Civil Society Coalitions & EU Actors

European civil society groups took a key step by forming the Coalition Against Unlawful Surveillance Exports (CAUSE) in 2014. This group unified the human rights-focused NGOs—Amnesty International, FIDH, Human Rights Watch, New America’s Open Technology Institute, Privacy International, Reporters Without Borders—that had been active on cyber-surveillance issues from the beginning.134 It showed that civil society recognized the importance of continuing to influence the implementation of the export controls at the EU level. It also showed a shift in focus from individual governments to EU bureaucrats and institutions. Their specific aim was the creation of “strict trade controls” based on the framework agreed at Wassenaar. The EU actors, including parliamentary representatives such as Marietje Schaake, and officials in the European Commission, the EU’s executive body, were the other key players in the debate in Europe post-2013. These officials worked closely with civil society and in many ways acted as norm entrepreneurs themselves.

Implementing Cyber-Surveillance Norms in Europe: The Policy Debate

Civil society shifted its attention to the implementation of the cyber-surveillance export controls in the European Union. In doing so, two main issues emerged. First, EU member states did not consistently enforce EU export controls on cyber-surveillance tools. Second, the Wassenaar controls only regulated a small subset of cyber-surveillance tools implicated in human rights abuses. These evident limitations involved tensions inherent in using export controls for human rights purposes. Both issues led the CAUSE group and other civil society actors to advocate for extensive reforms to the EU’s dual-use export control regulation. In another instance of norm

entrepreneurs grafting onto an existing policy process, they were able to get cyber-surveillanc“on board” the train of export control reform to ensure implementation of their norm.

First, the EU had an enforcement problem: under the existing dual-use regulation, member states could grant or refuse licenses with wide discretion. Although the EU had seemingly implemented the Wassenaar controls in 2014, its member states continued to permit the same cyber-surveillance companies to export their malware systems, even to the same countries in the Middle East where human rights concerns had motivated the rules. A document leak from Hacking Team in 2015 revealed that the Italian government granted it a “global license” for exports of its Remote Control System hacking software to Wassenaar members in November 2014. Denmark decided to relax its export controls and permit a subsidiary of BAE systems to sell surveillance tools to Middle Eastern regimes such as Saudi Arabia and Egypt. It was a widespread issue. A 2017 investigation by a group of Danish journalists found that European countries had granted dozens of licenses for surveillance technologies going to countries ranked ‘not free’ such as the United Arab Emirates since 2014. This problem was occurring “time and time again” in the words of journalists who wrote about the EU security industry.

Second, the Wassenaar export controls only addressed a narrow subset of cyber-surveillance technologies implicated in human rights abuses. And, they did not explicitly take human rights into account in the licensing process. As a report on cyber-surveillance tools described, numerous cyber tools enable surveillance, including lawful intercept systems, mobile telecom interception systems and digital forensics systems, were not covered under the Wassenaar controls. An authoritarian regime could have used any of these to monitor or target vulnerable populations for surveillance. But defining the specific technical characteristics of all cyber-surveillance tools is quite difficult, as extensively discussed in the debate over the export controls in the United States. Member states also lacked guidance on how they were to implement the controls, especially when human rights were concerned. Civil society groups described the assessment criteria as having a “vague nod” to human rights, which allowed the inconsistent enforcement described above.

These problems were not oversights in the EU’s implementation of the controls. In fact, they were inherent features of export controls. Dual-use export controls are intended for national

security purposes – for preventing goods with advanced military applications from unintentionally ending up in the hands of malicious states. The licensing process therefore attempts to balance between business interests and national security concerns. Human rights are not built into the system. For this reason, none of the existing EU criteria took them into account. And because national security is left to individual states, the export control system had few constraints to ensure EU-wide consistent policies.

By focusing on export control implementation, civil society groups ended up injecting themselves on the side of greater harmonization of export control policies at the EU level. They advocated for much stronger human rights protections to be put in place through a reform of the dual-use regulation. These points were a crucial part of CAUSE’s platform, which called export controls a “necessary and major component of any successful mitigation strategy” to protect human rights.\(^ {142}\) Previously, the key policy issues related to the dual-use regulation were concerns about its strength on weapons of mass destruction proliferation.\(^ {143}\) These discussions involved experts on arms controls and business leaders, not human rights NGOs or cybersecurity researchers. The fact of these new actors’ participation in this policy process was significant for both the direction of export controls and for how civil society shapes cyber technology policies. As regulators started to apply export controls to cybersecurity tools, it is a natural progression to add relevant expertise, such as the researchers who took a more active role in the U.S. context. The participation of human rights groups was novel — it was one of the first times that outside groups not focused on security or technical expertise weighed in.

With this new angle for export controls came a new potential approach to bridge the gap between national security and human rights: human security. This idea, which originated from UN efforts to build a concept of security that focused on threats to the individual such as famine, crime, disease, ethnic violence and terrorism, had become an important theme of the EU’s Common Foreign and Security Policy.\(^ {144}\) While vague, human security provided an approach for considering how cyber-surveillance tools enabled regimes to threaten individuals’ privacy and security. But, surprisingly, it was not an NGO that proposed applying human security to cyber-surveillance. In fact, it was the European Commission that first brought up the idea in its review of export control policies, saying it would consider “evolving towards a ‘human security’ approach recognizing that security and human rights are inextricably linked.”\(^ {145}\) Parliamentarians offered support for this approach, with MEP Bodil Valero arguing for prioritizing human

---


security by evaluating end-user countries.\textsuperscript{146} Marietje Schaake, the policy leader within the European Parliament on surveillance exports, called for the EU to adopt the human security approach in her 2015 comments to Commission’s policy review.\textsuperscript{147}

The idea of applying human security to export controls aroused opposition. A majority of exporters and other consulted organizations in the Commission’s review expressed reservations about the human security approach. Many worried it would harm the competitiveness of EU exports.\textsuperscript{148} Notably, the CAUSE group opposed using the term human security in the place of human rights, arguing that human security was “not well-defined and legally binding” in contrast to human rights.\textsuperscript{149} Of course, this did not mean that CAUSE was against including human rights protections in licensing assessment criteria or mandating that states consider human rights impacts of surveillance tools. They framed the issue in terms of precision, arguing that authorities like the EU Charter of Fundamental Rights provided much more clear and well-defined criteria for licensing decisions.\textsuperscript{150}

For civil society, human security seemed to be a red herring – a fuzzy concept that would not guarantee the human rights protections they had long worked to enact. In any case, the Commission never provided a detailed explanation of how a human security approach might differ from the inclusion of human rights criteria. The debate did show how CAUSE and other NGOs — both traditional human rights groups and online privacy organizations – integrated themselves into the EU export reform debate. They were the most prominent groups analyzing the Commission’s 2016 proposal for a reformed dual-use regulation. NGOs in the CAUSE group developed a number of recommendations for changes to the dual-use regulation and critiques of the Commission’s proposal. Their focus on this policy development process produced a number of recommendations that aimed to dramatically alter the dual-use system:

- **Applying human rights criteria in licensing cyber-surveillance exports:** CAUSE argued for a specific requirement that national licensing authorities assess the human rights implications of a proposed export in license decisions.\textsuperscript{151} Previously existing requirements required the denial of arms exports if there was evidence that the technology might be used for “internal repression.” But under the EU dual-use regulation, it was not clear if licensing authorities had to fully comply with those criteria since they

\textsuperscript{150} Ibid., 20.

- **A ‘catch-all’ control for cyber-surveillance tools:** Catch-all controls enable licensing authorities to require licenses for items not listed on control lists that authorities wish to control for their potential impacts. CAUSE argued that a dedicated catch-all mechanism for cyber surveillance tools was necessary to fully cover all types of cyber-surveillance tools.\footnote{Coalition Against Unlawful Surveillance Exports, “A critical opportunity: bringing surveillance technologies within the EU Dual-Use Regulation,” June 2015. \url{https://www.fidh.org/IMG/pdf/cause_report_final.pdf}} It also argued for revisions of the existing catch-all system since catch-all controls imposed by national license authorities did not then apply automatically to all other jurisdictions.\footnote{Marietje Schaake, “Written submission to public online consultation on the export control policy review (Regulation (EC) No 428/2009),” European Commission, 2015. \url{http://trade.ec.europa.eu/doclib/docs/2015/november/tradoc_154004.pdf}} This loophole meant that items covered by a catch-all in one member state might not require licenses in other states.

- **Introducing EU autonomous lists to control additional surveillance tools:** CAUSE argued for independent EU lists that would add more types of surveillance tools such as lawful interception equipment to the already-implemented controls from Wassenaar.\footnote{SIPRI and Ecorys, “Final Report: Data and information collection for EU dual-use export control policy review,” European Commission. November 6, 2015. 219. \url{https://www.sipri.org/sites/default/files/final-report-eu-dualuse-review.pdf}} Many EU government and industry officials opposed the adoption of an EU autonomous list because it could undermine the EU’s position in Wassenaar.\footnote{Marietje Schaake, “Written submission to public online consultation on the export control policy review (Regulation (EC) No 428/2009),” European Commission, 2015. \url{http://trade.ec.europa.eu/doclib/docs/2015/november/tradoc_154004.pdf}}


- **Elimination of controls on encryption technologies:** CAUSE argued that the EU should push for the eradication of the WA’s cryptography controls. Civil society groups had long opposed the restrictions on encryption. They linked encryption to protection of privacy and security of communications. A different group, the Center for Internet and Human Rights (CIHR) argued that the EU should adopt a general export authorization for cryptography, similar to an existing exception in the U.S.\footnote{Center for Internet and Human Rights, “Export Controls of Surveillance Technologies,” European University Vienna, 2015. \url{https://cihr.eu/wp-content/uploads/2015/11/Export-Controls-of-Surveillance-Technologies_DEF_BW.pdf}}
• **Country-specific lists:** Marietje Schaake argued that it would be effective to put in place lists of specific destination countries where the EU could impose ad hoc export controls on non-listed technologies.\(^{160}\)

• **Issuing non-binding guidance for corporate social responsibility:** Schaake and other experts also called for the EU to provide businesses with information about best practices such as due diligence so that companies could effectively self-regulate their behavior.\(^{161}\) In 2014, the UK issued guidance along these lines that civil society cited as evidence this approach could be effective for industry self-regulation.\(^{162}\)

• **Greater transparency for licensing applications and decisions:** CAUSE argued that increasing transparency requirements for national licensing authorities would make it easier to address inconsistent policies at the national level.\(^{163}\) Schaake also stated that member states should provide information to the Commission about the number and types of applications received.\(^{164}\)

CAUSE and other NGOs essentially proposed to adapt dual-use export controls to regulate the software trade: to empower states to block exports based on human rights concerns, even technologies not on export control lists and to constrain them from permitting exports of controlled technologies to known human rights violators. The policy outcomes from the EU thus far show a remarkable case of success for civil society on these issues.

**Analyzing the EU dual-use regulation reform measures**

The Commission’s initial proposal for a reform of the dual-use regulation adopted many of the proposals from civil society groups for specific controls on cyber-surveillance technology.\(^{165}\) Specifically, it added a definition of cyber-surveillance technologies under the broad umbrella of dual-use items and mandated the consideration of human rights criteria in export licensing decisions.\(^{166}\) The most consequential legislative change was the creation of a catch-all control that would apply for any items destined for users involved with “serious violations of human rights or international humanitarian law,”\(^{167}\) Instead of being a dedicated cyber-surveillance catch-all, this provision would have applied to any and all dual-use exports going to human


\(^{161}\) Ibid., 5.


\(^{166}\) Ibid., 19.

\(^{167}\) Ibid., 24.
rights violators. Additionally, the proposal included a general export authorization provision for encryption technologies but no specific exemptions for intrusion software security research.168

CAUSE saw the Commission’s proposal as good on the broad strokes but weak on the specifics. The proposal did not explain how national export authorities would determine which end-users were involved in human rights violations, include the requested exemptions for security research, or clarify how the catch-all would be applied in practice. BDI, a technology industry association representing German firms, argued against the catch-all, supporting instead country-specific lists.169 It also opposed the proposal’s introduction of an EU-specific list of cyber-surveillance tools beyond what was controlled through Wassenaar.170 The Commission’s proposal envisioned a broader human rights approach to export controls, expanding the EU’s power to regulate new technologies with the goal of preventing human rights abuses, not just specifically cyber-surveillance items.

In the European Parliament, Marietje Schaake offered her own set of amendments focused on cyber-surveillance tools. She argued against including cyber-surveillance tools within the category of dual-use items. Rather, she attempted to redefine the regulation as controlling both cyber-surveillance tools and dual-use items.171 She limited both the focus of the EU autonomous list to cyber-surveillance items only.172 And, Schaake redefined the intrusion software control and added exemptions for security research, along with totally eliminating the controls on encryption.173 Her amendments diverged from the Commission by attempting to impose more defined, tighter controls on cyber-surveillance items and by scaling back the scope of human rights-based controls for other technologies.

The final text adopted by the Parliament in early 2018 struck a middle ground between Schaake and the Commission. It did not separate cyber-surveillance tools from dual-use items as Schaake had done, but it did add a significant level of detail to the human rights criteria involved in licensing assessments, catch-all criteria and the reform’s overall justification.174 Like Schaake, it based the human rights assessment criteria on the EU Common Position 2008/944, and it limited the scope of the EU autonomous list to only cyber-surveillance tools.175 It also restricted the

---


170 Ibid., 15.


173 Ibid., 56.


175 Ibid.
human rights catch-all to only apply for cyber-surveillance tools. But it also added more requirements for any cyber-surveillance license, including that exporters have to provide an end-use statement describing the intended uses of the technology. It echoed Schaake’s approach when it came to transparency requirements and adding requirements for due diligence guidance, but diverged from her on encryption, stating that the Commission should submit proposals in a few years time on eliminating the cryptography controls.

Although the Parliament text did not totally follow Schaake’s changes, like her amendments, it focused the controls on cyber-surveillance tools while limiting the other human rights dimensions of the export control reform. The approaches of each proposed bill with regard to the above-listed policies are summarized in Table 3 below, noting support or opposition from key civil society actors, including previously mentioned groups and the technology association Digitale Gesellschaft EU (DGEU).


<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Supporters</strong></td>
<td>CAUSE</td>
<td>CAUSE</td>
<td>CAUSE</td>
<td>CAUSE, CHIR, MS, BDI, DGEU</td>
<td>CAUSE, CHIR, DGEU</td>
<td>SIPRI, MS</td>
<td>CAUSE</td>
<td>DGEU, BDI, MS</td>
</tr>
<tr>
<td><strong>Opponents</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Commission Proposal</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adds cyber-surveillance tech to dual-use definition</td>
<td>Controls cyber-surveillance tech used for serious human rights violations</td>
<td>Controls monitoring centers &amp; lawful interception</td>
<td>Committing to releasing guidance General Export to avoid burdening research activities</td>
<td>Authorization for encryption</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Separates cyber-surveillance from dual-use</td>
<td>Limits EU autonomous list to cyber-surveillance tech</td>
<td>Limits scope of intrusion software controls to protect research</td>
<td>Curbs scope of intrusion software definitions</td>
<td>Eliminates cryptography controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Marietje Schaake Amendments</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defines serious human rights violations</td>
<td>Similar scope to Commission’s catch-all</td>
<td>Removes ‘digital forensics’</td>
<td>Echoes Commission on issuing guidelines</td>
<td>Requires</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specifies consideration of right to privacy, data protection, rule of law in assessment</td>
<td></td>
<td></td>
<td></td>
<td>No country list</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defines who designates human rights violations, focusing human rights dimension on cyber-surveillance items</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Limits scope of catch-all to cyber-surveillance tech with connections to human rights violations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Limits of catch-all to cyber-surveillance tech with connections to human rights violations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Parliament Final Text</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defines due diligence</td>
<td>Explicit exclusion of testing/proactive research</td>
<td>Defines due diligence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Revises intrusion software definitions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**EU Export Control Reform & the evolution of cyber-surveillance norms discourse:**

The final EU policy on export control reform will not become law until 2019 at the earliest. At the time of writing, the Parliament and Commission text had gone into “trialogue” negotiations between the EU Council, Parliament and Commission – with the member states in the Council

---

176 Ibid.
now getting the chance for their say.\textsuperscript{177} The CAUSE group has thus far had a remarkable degree of success in integrating its proposals — such as a human rights criteria, a cyber-surveillance catch-all and EU autonomous lists — into the reform. Marietje Schaake, a highly effective legislator on the Parliament’s Foreign Affairs and International Affairs committees coordinated with the CAUSE group to advocate for their priorities. Remarkably, business groups like BDI and DGEU were not able to stop the inclusion of catch-alls even though they supported the broader focus on human rights.\textsuperscript{178} Industry associations had less power in the EU than their counterparts did in the U.S. simply because the U.S. has the largest group of cybersecurity companies.\textsuperscript{179} The lack of a strong opposition indicates broad acceptance of the norm against proliferation of cyber-surveillance tools to human rights violators. But civil society did not get everything they wanted: the EU Parliament deferred on removing cryptography controls.

The most successful proposals were those that narrowly focused their changes on cyber-surveillance tools. In this regard, the human security approach was a surprising failure on the part of the European Commission. Parliament largely rejected the Commission’s vague language that extended the human security approach to many types of dual-use technologies. Instead, the Parliament drew much more on clear human rights standards (as many NGOs called for it do).\textsuperscript{180} These decisions show a norm that is focused narrowly on a small subset of certain tools. This is a product of the CAUSE group’s choice to graft their proposed norm onto the existing export control framework, not, in effect, re-do the entire system to create a new organizational platform for cyber-surveillance regulation.

It is not clear whether the reform redirects the purpose of export controls towards preventing human rights violations that result from technology transfers. The Commission and Parliament leverage unusual tools for export controls like catch-alls and autonomous lists to specifically address the human rights impacts of cyber-surveillance tools. But the proposed policies do not use them for any broader human rights protection goal. Based on these limited impacts, it is not clear if or how export controls might be used for other human rights purposes in the future.

Finally, although the EU process may appear to reflect how civil society successfully pushed for the implementation of their norm, their focus on the EU level and cyber-surveillance specific controls may still yet provoke unintended consequences. The norm against surveillance proliferation received strong buy-in at the EU but not from its key ally in Wassenaar, the U.S. Other countries like Israel have significantly relaxed their controls on intrusion software (which they enacted pursuant to a law that automatically implements the Wassenaar lists) and other Wassenaar members like Russia or Turkey have provided no evidence of implementing the


controls. The EU’s adoption of its own strict controls on surveillance tools could undermine the common coordination at the heart of export control regimes like Wassenaar.

VI: Conclusions

Ultimately, the outcomes of the complex policy debates, regulations and international attention on the export of cyber-surveillance tools show that a norm is developing against their proliferation to human rights violators. This article has argued that this case is an example of civil society-led norm cultivation. This concluding section discusses why civil society groups succeeded to the extent they did, how their efforts adapted to the nuances of cyber-surveillance technologies, and what lessons cyber-surveillance can offer for creation of cyber norms generally.

First, civil society achieved its greatest success by grafting cyber-surveillance tools onto the existing Wassenaar framework for export controls, in part by framing them as ‘digital weapons.’ While this approach put in place controls on cyber-surveillance, it did not mean that the norm against exporting cyber-surveillance tools to human rights violators had achieved widespread acceptance, nor that the norm was in the ‘cascade’ phase of implementation. Rather, choosing Wassenaar intertwined regulation of cyber-surveillance technologies with national security concerns about the spread of exploits. Over time, as export controls proved to be an inadequate regime for controlling the vulnerability trade, only the human rights basis for controlling cyber-surveillance remained. In the EU, grafting onto dual-use export controls also enabled CAUSE to use it as a platform for their policy proposals.

Some norm entrepreneurs were more successful than others. Privacy International and other groups that focused on online privacy achieved many of their goals in the EU policy reform, as did the more traditional human rights groups Amnesty International and Human Rights Watch. The CAUSE group unified civil society in Europe, putting their voices prominently into the policy process over objections from technology industry groups like BDI. Yet no similar group formed in the United States. Security researchers, who formed a very different kind of civil society, had the most success in the U.S. context, even eventually contributing to the U.S.-led addition of vulnerability research exemptions to the Wassenaar controls.

Second, technical experts and researchers emerged as key actors that drove many normative and policy developments in the process. The Citizen Lab and security researchers like Sergey Bratus explained the powerful impact of both surveillance technologies and of overly broad export controls on ‘intrusion software,’ using incredibly well-supported technical evidence and analysis. The need for technical expertise modified state practices, as shown by the U.S choosing to send white hat hackers as part of its 2016 Wassenaar delegation. In the EU, NGOs like Privacy International and Access Now embedded technical expertise with their policy work. This helps explain the seeming absence of independent experts from the EU context. Combining technical expertise and policy advocacy proved highly effective for EU NGOs. As policymakers had little experience in crafting regulations for cyber technologies, discourse from technical experts — like the Citizen Lab’s research and American hackers’ explanations of software vulnerability research — were able to steer the debate towards their favored ends.

Both these conclusions point to an evolution in who and what people and groups “civil society” refers to: privacy-focused analysts and security-minded hackers whose work and advocacy both complemented and opposed the efforts of more well-established NGOs. And the NGOs that drove this process were relatively new ones – Access Now was founded only in 2009. This
evolution in what a norm entrepreneur looks like for cyber technologies was a key feature of the cyber-surveillance issue and one that highlights the expanded sets of actors with equities in cyber technology governance. Additionally, the new relationships that formed between civil society groups across issue areas was crucial for first framing the issue of cyber-surveillance and then forming cross-coalitions like CAUSE. These relationships will remain in place as civil society addresses new issues and evolves in response to the challenges of cyber governance.

Third, differences in process, information, and mobilized communities led to different policy outcomes in the EU and U.S. That is, in the U.S. the security research community advanced a more expansive vision of the scope of proposed intrusion software controls, a view that reached a cybersecurity-focused set of policy institutions. The norm had broad consensus, but in the U.S. the cybersecurity industry blocked the implementation of the norm because of the belief that the export controls applied broadly to offensive cyber tools, not that the norm itself was bad. This divergence led to different narratives (cybersecurity vs. human security) that applied to rhetoric about surveillance tools in the U.S. vs. EU. In the EU, civil society stayed active through the implementation of the Wassenaar export controls. This ensured that they were able to influence the evolving EU dual-use reform and could redirect it towards human rights. In the U.S., the security research community shifted the debate towards cybersecurity.

Fourth, the export controls were sufficiently complex and narrow such that they targeted a small set of technologies. The specificity of the controls increased as regulators added exceptions designed to exempt commercially available tools from the export controls. This form of regulation reflected the narrow nature of the proposed norm, which also recognized that law enforcement has legitimate uses for cyber-surveillance tools. Enforcing the norm through export controls required highly specific definitions and policies, a choice that reduced the actors that were willing to implement the norm but that also ensured states could observe how other states were implementing the norm in detail. This combination of the soft law of international frameworks like Wassenaar and the hard law of national export control regulations is a quite interesting example of how precise definitions can facilitate the dissemination of a targeted norm, a process that may be necessary with complex cyber-technologies.

Fifth, cyber-surveillance norms are not a simple story of success like the campaign to ban landmines. The end results of this over seven-year effort reveal some of the limitations of a civil society-led process and of export controls. States like Russia and China have their own robust cybersecurity industries and they are not limited by this norm. And the current divergence in policy between the U.S. and EU could undermine the effectiveness of global export controls. Technology-based controls will not address all possible means of cyber-surveillance because the systems evolve rapidly, nor will export controls categorically prevent authoritarian regimes from using surveillance to enable human rights abuses.

Especially because export controls are imperfect, it is important that export control policy function as well as possible. To improve current policy, the EU and the U.S. should work to resolve the differences in their export control standards, especially as the EU finalizes its dual-use reform bill in 2019. To that end, NGOs in the U.S. such as the EFF should join with the CAUSE group to focus their activism on the U.S. to push it to implement the Wassenaar controls and more comprehensively regulate cyber-surveillance tools. At the governmental level, EU countries should push for greater harmonization of controls through Wassenaar to ensure that the
Wassenaar controls are applied uniformly. Specifically, they should pressure the U.S. to implement the controls it agreed to at the 2017 meeting. EU countries should also take up the issue of encryption at Wassenaar and push for the removal of all export controls on cryptography, which helps give dissidents and journalists the tools they need to evade surveillance. This effort could serve as part of a compromise with privacy-focused NGOs in the U.S. like the EFF in order to secure their support for cyber-surveillance controls.

As we consider the future of cyber norms, we should broaden our ideas of the norm development process. These ideas should consider how norms develop through campaigns, frameworks and institutions not typically thought of as the right venues for building cyber norms. The story of the complex regulations, laws and debates about cyber-surveillance highlights how civil society, especially policy-focused NGOs and researchers can have a demonstrable effect on global cyber norms. Approaching the process of cyber norm development as an exercise in strategic social construction will shine more light on how lasting norms for cyberspace might come about. This article argues that in the case of cyber-surveillance tools, civil society leadership, grafting onto existing frameworks, narrowly targeted and highly specific rules, and technical expertise all played crucial roles in shaping the eventual policies regulating cyber-surveillance.

For cyber norms generally, this finding suggests that civil society norm entrepreneurs can have the greatest impact with highly targeted norms on either specific technologies or specific behaviors in cyberspace. Rather than creating new international platforms like the UN GGE, these norms might achieve more success if they build off existing frameworks — like existing technology control regimes or international conventions. Leading states constantly emphasize that cyberspace is not just for states but also for businesses, NGOs, universities, and individuals. Those actors should shape the rules that govern cyberspace. Even though civil society groups are by no means the most powerful or influential of these actors, with the lessons from defining cyber-surveillance norms they can have an outsize impact in building the rules for cyberspace.
Works Cited


Council Regulation No. 1236/2005 concerning trade in certain goods which could be used for capital punishment, torture, or other cruel, inhuman, or degrading treatment or punishment, L. 200, July 30, 2005. [Link]


DIGITALEUROPE. “DIGITALEUROPE Comments on the INTA vote on proposal for a recast of export control Regulation.” Brussels, November 23, 2017. [Link]

Electronic Frontier Foundation. “About EFF.” [Link]


https://dash.harvard.edu/bitstream/handle/1/12308565/Nye-GlobalCommission.pdf


https://www.nytimes.com/2016/05/30/technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html


https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-i-finfisher-and-amesys

https://publications.parliament.uk/pa/cm200809/cmselect/cmquad/178/17810.htm


http://www.un.org/en/sections/resources-different-audiences/civil-society/


