COUNTERING THE PROLIFERATION OF OFFENSIVE CYBER CAPABILITIES

Mr. Robert Morgus, *Cybersecurity Initiative & International Security Program, New America*

Mr. Max Smeets, *Centre for International Security and Cooperation (CISAC), Stanford University*

Mr. Trey Herr, *Harvard Kennedy School*

MEMO №2

TABLE OF CONTENTS

SECTION 1: INTRODUCTION

The tenor of the cyber stability debate, often moribund and moving more sideways than forward, changed with the 2010 United Nations Governmental Group of Experts (UN GGE) Consensus Report that international law applied to cyberspace.[164] It followed a position paper by the Obama administration published in January of that year to bring the various sides closer together. Though it wasn't a steep trend line which followed, the slow process towards cyber norms was considered to be meaningful and positive.[165]

Despite this and subsequent progress, however, the events of 2017 have shed doubt on this progressive dynamic. The collapse of the UN GGE process in June sent an alarming message that we are moving *away* from establishing a meaningful cyber stability regime, rather than towards it. Moreover, global cyber attacks, such as WannaCry and NotPetya, once again demonstrated the destabilizing potential of the proliferation of cyber capabilities.[166]

Norms and legal interpretations are one way to bring order to international society.[167] The purpose of this policy report is to offer a new set of recommendations, derived from a clear framing of the proliferation process and likely to contribute to meaningful progress toward cyber stability at the international level. Over the past decade a great deal of time, energy, and precious focus has been dedicated to developing norms of responsible behavior—what states and other international actors *should* and *should not* do in cyberspace. But this is only half of the conversation. Progress against proliferation must also consider what groups *can* and *cannot* do. In short, time is ripe to explore countering the proliferation of offensive cyber capability. This leads to our core research question: what are the key facets of the ecosystem that facilitates the proliferation of offensive cyber capability?

This policy report provides a framework for mapping the process of proliferation in cyberspace and its implications for states and policymakers, with the aim of understanding how to better counter it. In our analysis we introduce the Transfer-Actors-Capabilities-Effects (TrACE) framework, which helps to explain the dynamics of proliferation in cybersecurity and serves as an intellectual basis for counterproliferation efforts by the policy community. This framework captures how proliferation occurs between a diversity of actors and encompasses three overlapping activities: i) the purchase and sale of individual malicious software information and individual components that contribute to the development of offensive cyber capabilities, ii) continued research and innovation by a small set of

[164] Note that there were already already signs of this change in 2008. See: John Markoff, "Step Taken to End Impasse on Cybersecurity Talks," *The New York Times*, (July 17 2010) retrieved from: http://www.nytimes.com/2010/07/17/world/17cyber.html?mcubz=0.

[165] Michael Schmitt and Liis Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms", *Just Security*, (June 30, 2017), retrieved from: https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

[166] Victory Woollaston, "WannaCry ransomware: what is it and how to protect yourself," *Wired* (May 22, 2017), retrieved from: http://www.wired.co.uk/article/wannacry-ransomware-virus-patch; Andy Greenberg, "The Wannacry Ransomware Hackers Made Som Real Amateur Mistakes," *Wired*, (May 15, 2017), retrieved from: https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/; Lily Hay Newman, "Latest Ransomware Hackers Didn't Make Wannacry's Mistakes," *Wired*, (June 27, 2017), retrieved from: https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/.

[167] See Hedley Bull, *The Expansion of International Society.*

advanced states, and iii) the inadvertent transfer of capabilities—both sophisticated and not—to non-state groups and less capable states.

Applying the model to counterproliferation efforts, we indicate that *current* feasibility of international agreements is low. The implementation of export controls could weaken defense more than offense.[168] Also, arms control agreements are not conceived to be an effective path due to the current infeasibility of setting and enforcing standards of behavior. The feasibility of such interventions in the future, however, remains unclear.

We find that, in the short term, institutional tools that could be leveraged unilaterally or within like-minded coalition are more feasible. This includes the enhancement of both defensive and offensive capabilities, as well as the (further) implementation of a diplomatic toolbox.[169]

Our recommendations are therefore aimed at increasing the cost of developing offensive cyber capabilities, diminishing the utility of capabilities in the hands of troublesome actors once spread, and providing a way forward for meaningful action on increasing the barriers to actors transferring these capabilities.

The remainder of this report proceeds as follows. Section II sets out the scope of our analysis. Section III discusses the objectives in counterproliferation. In section IV, we provide an overview of the TrACE framework to explain cyber proliferation dynamics. Section V, in turn applies the TrACE framework to counterproliferation efforts, outlining a range of connected initiatives, tackling all processes within proliferation. The final part, Section VI, concludes and provides a list of recommendations for policymakers.

[168] Trey Herr, "Malware Counter-Proliferation and the Wassenaar Arrangement," in *2016 8th International Conference on Cyber Conflict: Cyber Power* (CyCon, Tallinn, Estonia: IEEE, 2016), 175–90, https://ccdcoe.org/cycon/2016/proceedings/12_herr.pdf.

[169] We note that the manipulation of the market through purchasing power will be more difficult in the current environment.

SECTION 2: SCOPE OF ANALYSIS

This section clarifies the scope of our analysis. The call for counterproliferation of offensive cyber capabilities is not new. Indeed, the potential control of "intrusion software" was embedded in the Wassenaar Arrangement aimed at "creating consensus approach to regulate conventional arms and dual-use goods and services."[170] Our approach differs significantly from previous efforts which primarily sought to counter cyber proliferation through imposing standards *like* Weapons of Mass Destruction (WMD) prevention programs.[171]

Although there may be valuable lessons to learn from the WMD approach, we argue that this approach on its own is *not* viable.[172] After all, cyber proliferation is embedded in a unique ecosystem of actors and information.[173] Previous efforts have focused on blocking the flow of cyber capabilities without developing a detailed understanding of the *mechanisms* of cyber proliferation. The starting point of our analysis is that we can only find ways to counter the spread of these capabilities if we know *how* they spread.[174] We also need to be much clearer about the objectives of a counterproliferation effort. While a "cyber-weapon-free" world is unlikely, it should provoke debate over what goals are feasible in the near to mid-term.

There are four assumptions underlying this paper. First, we assume that countering the proliferation of offensive cyber capabilities is a useful activity in the context of cybersecurity.[175] Moreover, we believe that counterproliferation is a *necessary* activity for the maintenance and improvement of international stability.

[170] See: "About us", Retrieved from: http://www.wassenaar.org/about-us/

For an excellent basic overview see: Cristin Flynn Goodwin and Brian Fletcher, "Export Controls and Cybersecurity Tools: Renegotiating Wassenaar," Marina Bay Sands, (July 20-22, 2016) retrieved from: https://www.rsaconference.com/writable/presentations/file_upload/fle1-r01_export-controls-and-cybersecurity-tools-renegotiating-wassenaar.pdf

[171] Also see Greenberg's review of Clarke and Knake's proposal of a 'Cyber War Limitation Treaty'. See: Andy Greenberg, "Weapons of Mass Disruption," *Forbes*, (April 8, 2010), retrieved from: https://www.forbes.com/forbes/2010/0426/opinions-cyberwar-internet-security-nsa-ideas-opinions.html; Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, (HarperCollins: 2010)

[172] Trey Herr, "Governing Proliferation in Cybersecurity," *Global Summitry* 2, no. 1 (July 2017), https://academic.oup.com/globalsummitry/article/doi/10.1093/global/gux006/3920644/Governing-Proliferation-in-Cybersecurity?guestAccessKey=f88e2727-737a-4be2-991e-a3696624b420.

[173] For a discussion of the limits of the 'cyberspace ecosystem' metaphor see: Alexander Klimburg, *The Darkening Web: The War for Cyberspace*, (New York: Penguin Press: 2017)

[174] Note that, in the case of the Wassenaar agreement, there was also said to be a lack of technical expertise—partially because governments had no prior history of engaging with issues related to cyber security. For similar point see: Goodwin and Fletcher, "Export Controls and Cybersecurity Tools"

[175] There has been a vivid debate on nuclear proliferation on whether 'more may be better'. Waltz' famous logic on why the spread of nuclear weapons likely contributes to further stability was based on a number of propositions: i) nuclear states can only score small victories due to a fear of escalation, ii) the escalation costs are extremely high; iii) there is

Second, we define “cyber weapon” narrowly in this context but recognize that any analysis of proliferation must take more than this tiny sub-set of capabilities into account. A cyber weapon is any software which can cause destructive physical effects.[176] Offensive cyber capabilities, which are a wider category of which weapons are a subset, may also include software which causes destructive logical or digital effects. Cyber proliferation refers to the intentional *or* unintentional diffusion of offensive cyber capabilities between actors to cause effects through information systems or networks. This means our analysis addresses a range of capabilities which, while not weapons by any reasonable definition, could be combined to create destructive effects.

Third, our analysis does not consider the tools or services used to propagate narratives in information and influence operations. However, the tools which are used to *obtain* confidential information leveraged in information and influence operations do fall under this discussion.

Finally, this counterproliferation approach is not meant to *replace* ongoing international activities around the codification and enforcement of normative behavior and the identification of deterrence structures. Instead, these two pillars work *in concert* with one another to reinforce global stability.

There are several factors which may change and thus impact this analysis. The examples and descriptions used in this framework represent a snapshot of what is currently known. As time progresses, more actors may enter the space and capability may develop to elicit new and previously unforeseen effects. Capabilities may become radically more destructive or accessible, actors who employ these capabilities may become less numerous, and the rise of computing platform vendors like Google and Microsoft could change the attacker/defender innovation cycle. Each of these changes would impact the levers used to influence proliferation and while none require radical change to our framework, we note them as potential sources of change for assumptions and descriptions of behavior in future. As these factors change, so too will factors that determine the feasibility of the counterproliferation applications of the framework outlined in the next section. Nonetheless, while the factors within the TrACE framework are malleable, the framework itself is designed to be an evergreen way of analyzing the proliferation ecosystem.

increased certainty about relative strength, and iv) outcome of war is more certain. Note that for the use of offensive cyber capability, these propositions are much less likely to hold; there is much less clarity on relative strength as well as the outcome of a cyber conflict. It is also unlikely that the use of offensive cyber capability is as destructive. See: Scott D. Sagan and Kenneth N. Waltz, *The spread of nuclear weapons : a debate*, (New York: W.W. Norton: 1995)

[176] For an alternative definition see: Max Smeets, “A Matter of Time: On the Transitory Nature of Cyberweapons,” *Journal of Strategic Studies*, (2017)1:28

SECTION 3: THE PILLARS AND OBJECTIVES OF COUNTERPROLIFERATION

This section lays out the two pillars of counterproliferation and several potential objectives. Norms, laws, and deterrence appeal to actors' perception of what they should or should not do—they only constrain behavior as far as the threat of retroactive retribution can. In some cases, actors with capability will deem the potential retributive cost low enough to still break the norm or law and not be deterred. Counterproliferation takes this construct one step further. Certainly, it also constrains behavior by affecting the decision calculus of potential adversaries—in ways similar to those of normative, legal, and deterrent structures—but a comprehensive approach to counterproliferation goes one step further. It seeks to also limit what adversaries are capable of doing—what they can and cannot do—by taking steps to limit the spread or development of capability.

Counterproliferation in the context of weapons of mass destruction (WMD) is conventionally defined as "[d]irectly forestalling, rolling back, or eliminating efforts to proliferate [a weapon, and preventing an actor that has already obtained the weapon] from realizing any benefit from owning or employing these weapons."[177] Based on the above definition, counterproliferation involves two pillars, which can be used to guide a discussion about countering the proliferation of offensive cyber capability.

The first pillar focuses on how actors can *prevent* the acquisition or transfer of a certain weapon technology. The goal in relation to this pillar could be one of three: i) slowing, ii) limiting, or iii) stopping the spread. Regardless of the goal, this pillar does not only seek to address the spread of the finished product, but also to disrupt the independent development of capability and the spread of components that enable said development.

First, *slowing* the spread implies that spread is undesirable, but inevitable, so action is taken to forestall the development or acquisition of capability by a diverse set of actors. In conventional terms, an example of such an effort are the initiatives to stem the flow of small arms.

Second, *limiting* the spread implies that a certain subset of actors can be trusted to utilize the capability or material implicit in the capability responsibly. In these cases, efforts are made to block the transfer of capability to certain actors, while transfer to others is deemed acceptable. The efforts by the Non-Proliferation Treaty to stymie the flow of nuclear technology to states beyond those who initially developed it are a contemporary example of such an initiative.

Third, *stopping* the spread means halting any and all spread. In conventional terms, we might think of nuclear nonproliferation efforts as absolute prevention. The goal of these initiatives is to ensure that no form of nuclear capability spreads to any actor that does not already possess it.

[177] Justin Anderson, Thomas Devine and Rebecca Gibbons, "Nonproliferation and Counterproliferation," (March, 2014), retrieved from: http://oxfordindex.oup.com/view/10.1093/obo/9780199743292-0026

The second pillar focuses on how to reduce the utility of offensive capabilities already in the possession of an actor.[178] Changing this utility aims to shape decision calculus of those actors who would deploy it. There are many ways the decision calculus of an actor can be affected. This includes making it more difficult for an actor to deploy a capability, bolstering defenses to make the capability less impactful once deployed, and communicating the potential consequences of deploying a capability to one's adversary.

[178] There is no agreed upon definition of the terms "counterproliferation", "nonproliferation", and "arms control".

SECTION 4: THE TRACE FRAMEWORK

This section lays out the TrACE Framework, a parsimonious conceptual model to describe the key elements of proliferation: Transfers, Actors, Capabilities, and Effects. The purpose of the framework is to identify critical nodes in the proliferation process which provide opportunities for constructive intervention. The basic features of the framework are provided in *Table 14: Summary of TrACE framework*. What follows here is a more detailed description of each element. Along with the description of the particular components of the framework and their subcategories, we provide a non-exhaustive set of examples intended to develop better understanding, but not to provide an exhaustive or even extensive list of all known examples.

Transfers refers to the actual spread of capabilities between actors. These transfers can be *intentional* or *unintentional*.[179]

Intentional transfers describe a purposeful transaction or exchange. These could be ephemeral, as with a conference presentation, or tangible, like the rental of a botnet or the government purchase of surveillance malware from a company like BlueCoat.

Table 1: Examples of Intentional Transfer

Example	Explanation
Legitimate business sales	In some cases, companies are permitted by local laws to develop and sell what could be considered offensive cyber capability.
Criminal transfers	Criminal forums like Silk Road and AlphaBay facilitate the underground market for offensive cyber capability.
Transfers at conferences like BlackHat, DefCon, Chaos Community Congress	Sometimes, presentations at conferences or online seminars spread information about offensive capability. The intention of these presentations is generally not to spread capability to nefarious actors, but instead to prove the possibility of something to garner attention from defenders to craft fixes.
Transfers between states	Though little evidence suggests that states actively share or transfer cyber capability to one another, some traditional military and intelligence alliances are exploring avenues to do share capability.

Unintentional transfers refer to capabilities discovered and obtained through their use, such as through forensic analysis of a piece of malware, or through leaks.[180]

[179] Trey Herr, "Governing Proliferation in Cybersecurity," *Global Summitry* 2, no. 1 (July 2017), https://academic.oup.com/globalsummitry/article/doi/10.1093/global/gux006/3920644/Governing-Proliferation-in-Cybersecurity?guestAccessKey=f88e2727-737a-4be2-991e-a3696624b420.

Table 2: Examples of Unintended Transfer

Example	Explanation
ShadowBrokers	Capabilities discovered via a leak or a breach of internal security.
Duqu 2.0	Capabilities discovered through reverse engineering of previously deployed capability.

Actors are the entities responsible for developing, deploying, and defending against malicious capabilities. Our framework differentiates actors not based on their "stateness", but instead on their functional role. Thus, we break actors into four categories: (1) developers, (2) defenders, (3) enablers, and (4) deployers. In many cases, individual actors or entities fit into more than one of these categories.[181] For example, well-resourced nation states can be all the above, and an individual with meager means could be a developer. Consider the, at times, countervailing incentives within the American NSA; the agency has a long and storied defensive cybersecurity mission while being simultaneously responsible for executing signals intelligence collection and supporting US Cyber Command through the development, maintenance, and deployment of offensive cyber capabilities. Developers might also be defenders, nearly all of the software vendor community for instance, develops code but also works to defend it. In this analysis, we focus on developers of malicious capability to explain this taxonomy.

The traditional state/non-state distinction is lacking in this discussion, in part because there is little uniformity in the capabilities and behavior of all states or all non-state groups. Both states and non-states play different roles in the supply and demand of offensive cyber capabilities and related tools. While the legal status of states clearly differs from non-state groups, this is of little difference in our analysis of incentives, intentions, and behavior. The discussion of some non-state groups as proxies working on behalf of states is a attribution and control issue which presupposes little about the capacity of these groups or the source of their capability. The variation in proxy models means this would do little for our analysis as a standalone category.

Developers, in the context of the TrACE framework, are groups and individuals that manufacture and help maintain *offensive* capabilities including knowledge and software. These include individual researchers, national intelligence agencies, companies like Hacking Team, and even some criminal groups (though many are deployers rather than developers). Where a relatively few, well-resourced developers can produce robust capabilities from scratch, others patch together capability based on openly available or leaked information.

Table 3: Examples of Developers

Examples	Explanation
U.S. Cyber Command, GCHQ, German Cyber and Information	Intelligence agencies and military commands are key developers of offensive cyber capability. Many states have declared intention to develop robust offensive capability, though it is unclear

[180]For discussions see: Steven M. Bellovin, Susan Landau, and Herbert S. Lin, "Limiting the undesired impact of cyber weapons: technical requirements and policy implications," *Journal of Cybersecurity,* 3:1(2017)59-68; Ben Buchanan, "The Life Cycles of Cyber Threats," *Survival: Global Politics and Strategy*, 58:1 (2016)39-58

[181] Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (Rand Corporation, 2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

Space Command	how many have been successful.
NSO Group, Gamma Group, Hacking Team	A small group of private companies work closely with intelligence and law enforcement agencies to develop and ultimately sell offensive capabilities.
Paras Jha, Josiah White, Dalton Norman (all of the Mirai botnet), and Robert Tappan Morris (Morris worm)	Sometimes individuals will develop offensive capability. Sometimes these individuals will use these tools for personal gain or to prove a point. Other times they may release them unintentionally.
Russian Business Network, Yanbian Group, Hellsing, Carbon, Spiker/Carbanak	Some criminal groups are purported to have developed cyber capabilities on their own. In some cases these capabilities are sold or loaned out. In others, the criminal groups leverage the capabilities themselves.

Enablers are the groups and individuals that maintain a capability or facilitate its transfer. These can often be developers as well as covert groups like exploit brokers who are not developing or deploying a capability. These middlemen most often reside outside of government, whether companies like ReVuln and Vupen or criminal groups, such as those operating forums like AlphaBay.[182]

Table 4: Examples of Enablers

Examples	Explanation
AlphaBay, Hansa, Silk Road, Silk Road 3.0, Russian Anonymous Marketplace	Online message forums, often on the deep or dark web, provide platforms that enable the black market exchange of "goods" like vulnerabilities, completed capabilities, and tailored solutions.
Zerodium, Vupen	Some companies also provide a middleman service for individual and groups that possess vulnerabilities or capabilities to broker sales to willing and able buyers.

Defenders are the groups and individuals that try to prevent capability from having its intended (or indeed any) effect. As with the previous two categories of actors, defenders reside both in government, like the network of national computer emergency response teams, and outside of government, like independent security researchers, security vendors, and software and hardware manufacturers. While defenders ideally do not play a role in intentionally proliferating offensive capability, they play a potentially crucial role in countering the proliferation of offensive capability, as explained below.

Table 5: Examples of Defenders

Category	Example	Explanation
CSIRTs	JP-CERT, GovCERT Austria, CanCERT, CNCS	Increasingly governments around the world are developing computer security incident response teams (CSIRTs). The competencies and roles of these teams vary widely, but in most cases, CSIRTs housed in governments provide defensive services for government systems and critical infrastructure.

[182] Kurt Thomas et al., "Framing Dependencies Introduced by Underground Commoditization," 2015, http://damonmccoy.com/papers/WEIS15.pdf.

Security Researchers	H.D. Moore, Natalie Silvanovich	Independent security researchers play a crucial role in improving security by discovering and reporting vulnerabilities as well as other activities.
Software Companies	Microsoft, Oracle, SAP, Adobe Systems, Amadeus IT	The software industry is a key player in the defensive ecosystem. Some companies actively test their software for weakness and nearly all prominent software providers engage in the market for software vulnerabilities, sometimes paying outside researchers
Cybersecurity Vendors	Symantec, McAfee Check Point Software Technologies, Kaspersky Labs, Fox-IT,	Cybersecurity vendors provide products and services intended to reduce an organization's 'cyber risk'.
Cyber Commands and Intelligence Agencies	GCHQ, Dutch Cyber Command	Just as military cyber commands and intelligence agencies can and often are developers of offensive capability, many of these organizations are also tasked with defensive activity.

Deployers are the myriad individuals and organizations, from hacktivists to nation-states who use these capabilities. Some deployers are able to independently develop capabilities but many acquire components if not entire capabilities through transfer.

Table 6: Examples of Deployers

Category	Examples
Intelligence Agencies	The United States' NSA, Russia's Main Intelligence Directorate (GRU), GCHQ
Military Cyber Commands or equivalent units	U.S Cyber Command
Law Enforcement Agencies	U.S. Federal Bureau of Investigation
Criminal Groups	The Russian Business Network, Matsnu Gang, Zeus Gang, actors behind 'Operation Ghoul'
Individuals	Albert Gonzalez, Max Vision, Michael Calce, Jonathan James, Sven Jaschan, Kevin Poulsen, 'Kuji', 'Datastream Cowboy', Ehud Tenebaum, David Smith

Capabilities refers to the objects of proliferation, whether the knowledge behind a new tactic, the infrastructure used to support the deployment of capabilities, or the software deployed on a computer to have an effect. Capabilities are not monolithic, nor are they easily parsed. We frame capabilities as four related and sometimes overlapping components: knowledge, tools, infrastructure, and platform.[183]

Knowledge, like a software exploitation technique, is important in cyber security, more instrumental even than in traditional kinetic domains.

[183] Scholars attempting to do this include: Dale Peterson, "Offensive Cyber Weapons: Construction, Development, and Employment," *Journal of Strategic Studies*, Vol. 36, No. 1 (2013); Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security,* 41:3 (2016/17):72-109: Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, 22: 3 (2013)365– 40.

Table 7: Examples of Knowledge

Example	Explanation
Software vulnerability or exploit	Vulnerabilities in software and hardware exist, but the information on what they are and how to utilize them (exploits) can be seen as similar to a commodity.
Information about a physical system	Information about a physical system is integral in the development of cyber capabilities that try to affect physical infrastructure to cause damage or disruption.
Passwords or personal information	Breached passwords and personal information are often the means by which nefarious actors enter into systems they should not have access to, allowing them to carry out an attack.
The Art of the Possible	Sometimes, the simple depiction of what is possible is enough to spawn a new line of development of offensive capability.

Tools take this knowledge or a particular function and embody it in software. These might be tools to develop offensive capabilities or limited-use malware.[184]

Table 8: Examples of Tools

Example	Explanation
Acunetix	A web vulnerability scanner which focuses on web applications.
John the Ripper	A well known password cracker
Metasploit	A package of tools to determine which exploit to use (and how to configure it) as well as payload to use (and how to configure it).

Infrastructure describes connectivity resources like hosting and bandwidth as well as compromised computer networks like botnets and command & control servers used to sustain the operation of an offensive capability.

Table 8: Examples of Infrastructure

Category	Example	Explanation
Test Infrastructure	None publically available	In many cases, to achieve physical effects through cyber means, an attacker or attackers will need to possess nuanced understanding of how a physical system they plan to attack works and how different code injections will impact that system. To do so, some more well-resourced actors have been suspected of building test facilities with systems that mirror those they plan to attack.
Command and control infrastructure	CloudMe accounts used to communicate with recent Red October malware.	Command and control infrastructure is the infrastructure an attacker uses to conduct the attack.

[184] On the relationship between knowledge and tools in this context see: Slayton, "What Is the Cyber Offense-Defense Balance?"

Platforms range from from narrowly tailored tools like the Dridex banking trojan to the Equation Group espionage malware.[185] The most multi-featured and intricate appear to generally be a product of a small group of advanced states but there is no strict correlation.

Table 9: Examples of Platforms

Example	Explanation
Project Sauron	"[A] top-of-the-top modular cyber-espionage platform in terms of technical sophistication, designed to enable long-term campaigns through stealthy survival mechanisms coupled with multiple exfiltration methods," as Kaspersky Lab describes it.
BlackEnergy	An evolving set of Russian espionage malware, likely originally developed by criminal groups and later employed in attacks against Ukraine's power infrastructure. BlackEnergy is designed to execute "tasks" that are commissioned by its Command & Control servers and implemented by the plugins.

Effects are the changes produced on a computing system or attached hardware because of a capability's operation. These operations impact a system's confidentiality (its ability to keep data secret to certain people), availability (its ability to keep data or services available to users), or integrity (its ability to guarantee that data has not been changed or manipulated to produce an unintended effect).

Effects can fall on a spectrum, from access, through espionage and theft, to disruption, and ultimately destruction.

Access suggests a capability can operate on a computer system but implies no effects to change the system like an intelligence agency preparing a system for later operations. One example is the use of tools like Duqu to establish a digital beachhead on computer networks, in preparation for future activity like espionage. We define access as an effect because of the political significance of detecting an unauthorized actor in a computer network. Even without changing anything about the network, the presence of software like this can motivate crisis response and communicate substantial vulnerability.[186]

Table 10: Examples of Access Effects

Example	Explanation
Bowman Avenue Dam	In 2016, an Iranian hacker was able to remotely penetrate the back-office systems for a small dam, merely to gain information without attempting to influence the dam's operation.

[185] See Nikita Slepogin, "Dridex: A History of Evolution" *Kaspersky Lab,* (May 25, 2017), https://securelist.com/dridex-a-history-of-evolution/78531/.

and Ben Buchanan, "The Legend of Sophistication in Cyber Operations," Belfer Center White Paper (Cambirdge, MA: Harvard Kennedy School, January 2017), https://www.belfercenter.org/sites/default/files/files/publication/Legend%20Sophistication%20-%20web.pdf.

[186] DHS/ US CERT, "Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors," accessed November 12, 2017, https://www.us-cert.gov/ncas/alerts/TA17-293A.

Espionage & Theft compromises confidentiality and extracts data or information from a computer system for the attacker's gain. For example, the Red October malware was a multifaceted Russian espionage platform designed to siphon information from business, universities, and some government agencies.[187]

Table 11: Examples of Espionage & Theft Effects

Example	Explanation
OPM Hack	In 2015, Chinese hackers breached the computer system of the U.S. Office of Personnel Management (OPM), stealing key security clearance information on U.S. personnel.
Moonlight Maze	During the late 1990s, Russian hackers (Carberb) targeted US military information (technical research, contracts, encryption techniques, unclassified specifications of US war-planning systems) on the Pentagon, Department of Energy, NASA, private universities, and research labs' networks.
SWIFT Heist	Using the Dridex malware, unknown hackers (believed by some to be North Korean in origin) compromised the computer systems of several banks around the world and rerouted funds using vulnerabilities in the SWIFT system.
Anthem	A group based out of China, according to FireEye, were said to be responsible for a medical breach of information of Anthem. Although the CEO of Anthem said it was a 'very sophisticated' attack, other indicators suggest that it did not take anything extraordinary to compromise the systems.

Disruption compromises availability. Disruption can be as little as harassment or pose substantial risks to the stability of the Internet when it targets critical resources. The Mirai botnet, a collection of Internet of things (IoT) devices collected into a swarm, was used to target journalist Brian Krebs as well as disrupt internet availability and the domain name service (DNS) in 2016 and is a stark example of *disruption*.[188]

Table 12: Examples of Disruption Effects

Example	Explanation
Dyn, Estonia, Georgia,	Distributed Denial of Service (DDoS) attacks are an increasingly common form of disruption. The scale of DDoS attacks varies widely from rendering a single webpage inoperable to shutting off large swaths of the internet.
Witty Worm	An unknown actor wrote an exploit code, exploiting a vulnerability just two days after it was disclosed, with a destructive (lagged) payload
NotPetya	Ransomware is another increasingly common disruption effect that encrypts locks a user out of a computer or computer system until a bounty is paid to the attackers. Although early iterations of ransomware were reversible (the attackers could unlock the infected system upon receipt of payment), recent iterations have been less forgiving (in other words, they more function like wipers).

[187] Kaspersky, "'Red October' Diplomatic Cyber Attacks Investigation," SecureList, January 14, 2013, http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation#5.

[188] Ben Herzberg, Dima Bekerman, and Igal Zeifman, "Breaking Down Mirai: An IoT DDoS Botnet Analysis," *Incapsula Blog* (blog), October 26, 2016, https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html.

Destruction compromises integrity. This last category, destruction, can escalate, from integrity violations like damaging a file system, to wiping data, or even manipulating attached hardware to cause physical destruction. Destructive effects are the least frequent but most discussed effect on this spectrum. These operations include manipulating digital systems to cause physical effect but also a range of data destruction activities. These include the Stuxnet campaign and the crippling of a German steel mill in 2014 but also incidents like the Shamoon wiper attack against Saudi Aramco and Rasgas and the Dark Seoul wiper attacks against South Korea. [189]

Table 13: Examples of Destruction Effects

Example	Explanation
Stuxnet	In at least one case, cyber capability has been deployed to disrupt weapons programs, as was the case with the Stuxnet campaign, which caused physical damage to the Iranian nuclear enrichment facility in Natanz
Sony Pictures, Saudi Aramco	In both the Sony Pictures and the Saudi Aramco cases, hackers gained access to corporate computer systems and rendered machines inoperable using variants of wiper malware.

Capabilities leveraged to create such effects on confidentiality are often rudimentary and differ generally in terms of their level of obfuscation or covertness. Moving up the scale to disruptive effects, things like distributed denial of service attacks are common. Some of these are handled daily by major content delivery networks (CDNs) like Akamai.[190] Others have such marked impact that they occupy the public consciousness as with the Mirai botnet when it targeted a major domain name service (DNS) provider.

Table 14: Summary of the TrACE framework

	Transfers	Actors	Capabilities	Effects
Definition	The transfer of capabilities, knowledge, infrastructure, resources, or techniques between actors.	The entities responsible for developing and deploying malicious capabilities.	The software tools, techniques, or tradecraft used to produce some effect on a computer system.	The change produced on a computing system or attached hardware as a result of a capability's operation.
Categories	i) Intentional ii) Unintentional	i) Developers ii) Enablers iii) Defenders iv) Consumers	i) Knowledge ii) Tools iii) Platform iv) Infrastructure	i) Access ii) Espionage iii) Disruption iv) Destruction

[189] CFR, "Cyber Operations Tracker," https://www.cfr.org/interactive/cyber-operations.

[190] Buyya, Rajkumar, Mukaddim Pathan, and Athena Vakali, eds. "Content delivery networks", *Springer Science & Business Media*, 9 (2008), retrieved from: https://pdfs.semanticscholar.org/6ba0/658e77f3502a5f050b73d0cfbf2a571d0714.pdf

SECTION 5: MAKING PROGRESS ON PROLIFERATION: APPLYING THE TRACE MODEL

This section discusses the TrACE framework and uses it to offer guidance on how to counter the destabilizing effects of cyber proliferation. As said, counterproliferation implies a range of connected initiatives aimed at limiting, slowing, or stopping the spread of capability and diminishing its utility. Here, using the TrACE framework as guidance, we describe some possible counterproliferation activities in the context of cybersecurity and discuss their viability and current challenges. Several of these efforts exist, either directly or in more limited form.

Based on the TrACE Model, we now discuss the possible goals of proliferation and offer a series of recommendations. The first three elements of the TrACE model connect to Pillar I (transfer), while the last element of the model, effects, connects to Pillar II (utility). Though a comprehensive understanding of the model is required, we can now look at these elements individually because different interventions address different actors.

POTENTIAL INTERNATIONAL AGREEMENTS

Considering the first element, transfers, we focus on the *enabler* portion of actors. The second element, actors, does not apply in this context. The third element, capabilities, focuses on *developers* and *deployers*. For the final element, effects, we focus on *deployers*.

Non-cyber initiatives, which seem to be applicable to cybersecurity tend to address only one or two elements of the TrACE model. With this understanding, we can consider how conventional interventions relate to each of these elements and actors. Most prominently, for example, export control agreements would affect the *enablers*. Arms control addresses *developers*. One could also consider models for drug transfer controls and disease control, which would relate to *deployers* and *enablers*. Here, however, we focus on two types of international agreements: export controls and arms control. More research is needed to explore the potential utility of other international agreements, like law enforcement agreements (looking at drug enforcement as a potential model), disease control, or climate change.

In this context, we explore how an international agreement of any sort could apply to one or all elements of the TrACE framework. A successful international agreement requires the following features. First, it must be able to set a clear threshold or guideline for what is tolerated or not under the agreement. Second, it requires monitoring and verification of adherence. Third, there needs to be the potential for punishment if an actor fails to comply.[191]

[191] In some international discussions, the argument is made that actual punishment may not be required as long as the threat of punishment exists.

Table 15: Essential Features of International Agreements and the TrACE Framework

	Tr	A	C	E
Which actor does it address?	Enablers	NA	Developers	Deployers
Threshold - Long Term Feasibility	Yes	NA	Yes	Yes
Threshold - Short Term Feasibility	Low	NA	Low	High
Monitoring and Verification - Long Term Feasibility	Yes	NA	Yes	Yes
Monitoring and Verification - Short Term Feasibility	Low	NA	Low	High
Punishment - Long Term Feasibility	Yes	NA	Yes	Yes
Punishment - Short Term Feasibility	High	NA	High	High

Currently, traditional tools to limit the spread of capability, like export controls and arms control, are lacking in these areas in the context of cybersecurity. The deficiencies of ongoing international norms deliberations mean that the international community lacks clear consensus on thresholds or guidelines for what is and is not acceptable. A clear definition of these thresholds is a necessary prerequisite for meaningful application of export or arms control. The covertness of offensive cyber programs poses challenges for monitoring and verification. Finally, as with many international agreements, more work must be done to identify meaningful punishment for defectors or those who choose not to comply. Here we outline these and other shortcomings in more detail and offer a series of challenges that must be addressed before such international interventions reach a threshold of feasibility.

ARMS CONTROL AGREEMENT

Arms control agreements could most readily apply to states developing capabilities, aimed at limiting or entirely banning this development activity. Progress through such agreements is likely to be limited and would likely require clarity on existing standards of behavior like the development or use of destructive offensive capabilities.

While not directly pointed at addressing the *transfer* of capability, an arms control agreement would target the development of capability. An arms control agreement for offensive cyber capability would involve states (possibly with other *developers*) agreeing to cease the production of either segments of or all offensive capability. Contemporary analogues for this type of intervention include the Chemical Weapons Convention (CWC), the Ottawa Landmine Treaty (Ottawa Convention), and Biological Weapons Convention (BWC). Yet, there are several challenges.[192]

Kenneth Geers examined the feasibility of a Cyber Weapons Convention based off of the CWC, pointing to the convention's success in minimizing the use of chemical weapons, which has drastically fallen since WWI when chemical

[192] Including where an arms control agreement could raise uncertainty about or, at worst, outright ban some defensive activities like penetration testing and vulnerability reporting.

weapons caused one third of casualties.[193] He concludes that three characteristics that make the CWC so effective apply to a cyber arms control regime: (1) political will , because the threat posed by cyberattacks is sufficiently severe worldwide for political consensus on the issue; (2) universality, because "everyone is a neighbor in cyberspace," which naturally lends itself to shared or universal goals; and (3) sufficient assistance, because an organization dedicated to helping member states improve their cybersecurity situations is feasible. While these conditions may be feasible in the long run, all three are currently absent.

At a basic level, an international arms control agreement is likely only effective when it is agreed to by the biggest *developers* of offensive capabilities. Even if we assume the most prominent of these developers are nation-states—an uncertain characterization given the sophistication of some non-state groups—we face a definitional challenge: what is a cyber weapon? Some states conflate information weapon and cyber weapons, viewing tools that enable the propagation of narratives or news as cyber weapons, while others define them as only tools that manipulate computer hardware and software.[194] Meaningful progress on bridging this divide is a prerequisite to an effective arms control arrangement.

Even if there were ready definitional agreement, the problem of political will remains. As alluded to above, landmines, chemical, and biological weapons are the major precedents. They share a common trait in that they are viewed as morally abhorrent for either their blatant inability to distinguish between targets (landmines) and the existence of more humane means to achieve the same or similar military ends (chemical and biological weapons). In short, they clearly breach international humanitarian legal principles of distinction and necessity. Although some capabilities do not distinguish between legitimate military targets and non-targets, to some, cyber capabilities are seen as perhaps the most humane tool to achieve military ends due to their non violent nature.[195] Arms control only works if the major players agree to cease production and use. It is exceedingly difficult to picture a world in which the political will would exist to create an arms control agreement for any current capability. Depending on how cyber capabilities evolve, this could change, and that change will be driven by *effects*.

The final challenge is a purely operational one: how and by whom would such an agreement be verified? The BWC and Ottawa Convention both lack formal verification and compliance mechanisms. However, the CWC does provide a potential model for verification through the permanent Office for the Prohibition of Chemical Weapons (OPCW). The OPCW is similar to the better-known International Atomic Energy Association, in that it is a permanent international organization that "includes a verification division with an international corps of about 180 inspectors who travel to declared military and industrial sites around the world."[196] The CWC model also shows promise as an analogue for a cyber arms control agreement because the two technologies share one crucial trait: the material and knowledge leveraged to develop capability both change quickly as new discoveries are made and are dual-use. The CWC addressed this arms control challenge by creating and consistently updating a scheduling apparatus to identify the most potentially harmful types of chemicals.

[193] Kenneth Geers - Cyber Weapons Convention, http://www.sciencedirect.com/science/article/pii/S0267364910001081

[194] See, for example, the conflation of cyber and information security in the repeated calls for a Code of Conduct for Information Security by several Shanghai Cooperation Organization states. https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf

[195] Tim Maurer - "The Case for Cyberwarfare," *Foreign Policy,* http://foreignpolicy.com/2011/10/19/the-case-for-cyberwarfare/

[196] Jonathan B. Tucker - "Verifying the Chemical Weapons Ban: Missing Elements," *ArmsControl Association*, https://www.armscontrol.org/print/2289

EXPORT CONTROL ARRANGEMENT

Though export controls hold some promise for countering the proliferation of offensive cyber capabilities, the sloppy application of the tool threatens defense as much or more than offense.

An export control arrangement would harmonize the export controls of nations *developing* or harboring *developers* to limit the *transfer* of *capabilities* or the means to develop capabilities to a set group of nations. The counterproliferation opportunity associated with an export control arrangement resides in preventing the spread of capability from agreeing *developers* to a group of identified state, corporate, and/or individual consumers. To provide an analogue, export controls are an important tool in the implementation of the Nuclear Nonproliferation Treaty (NPT) through the Zangger Committee.[197]

However, export controls face a number of challenges in the context of cyber counterproliferation. First, an export control arrangement does not ban the proliferation of capabilities within states. Second, at a fundamental level, export controls only restrict the flow of goods and services in white markets. As at least a portion of interstate *transfer* already occurs on black markets, this will not necessarily pose a new challenge, but it is likely to increase the challenge. In addition to these challenges, the use of export controls in the context of cyber proliferation poses two discrete risks. First, overly inclusive controls could place detrimental limits on spreading defensive technology and information. Second, export controls tend to push trade in materials to black, less visible markets.

Controls proposed via the Wassenaar Arrangement, a 41-member multilateral export control regime, was an initial foray into the use of export controls to limit the spread of cyber capability and starkly illustrates these risks and challenges. Indeed, the "intrusion software" control, proposed by the British delegation, was initially framed to focus on "Advanced Persistent Threat Software (APT) and related equipment (offensive cyber tools)."[198] The purpose of the proposal was to harmonize the export controls of Wassenaar members to limit the spread of intrusion software, but the ongoing controversy around the control starkly demonstrates one of the potential risks, that of over inclusiveness, as discussed here.

The intrusion software control used broad language in an attempt to capture as much malicious capability as possible. However, in doing so, this overly inclusive definition had the unintended consequence of also limiting defenders. Indeed, many in industry and academia fear that the restrictions could also apply to benevolent pursuits like penetration testing and information sharing on vulnerabilities, as the language of the control does not differentiate based on intent.[199] In addition to the concerns of security companies that the controls would restrict their ability to do

[197] Nuclear Threat Initiative. "Zangger Committee (ZAC)." *Nuclear Threat Initiative*. http://www.nti.org/learn/treaties-and-regimes/zangger-committee-zac/

[198] Reports from the Business, Innovation and Skills, Defence, Foreign Affairs and International Development Committees Session 2013-14 Strategic Export Controls: Her Majesty's Government's Annual Report for 2011, Quarterly Reports for 2011 and 2012, and the Government's policies on arms exports and international arms control issues; Response of the Secretaries of State for Defence, Foreign and Commonwealth Affairs, International Development and Business, Innovation and Skills, para. 88, October 2013. http://www.official-documents.gov.uk/document/cm87/8707/8707.pdf (p. 37)

[199] Sergey Bratus et al., "Why Wassenaar Arrangement's Definitions of Intrusion Software and Controlled Items Put Security Research and Defense At Risk—And How To Fix It" (Public Comment, October 9, 2014), http://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf.

business,[200] security researchers harbored concerns that these controls would prevent penetration testers in countries that implement controls from responsibly reporting vulnerabilities discovered across borders. In short, the over inclusiveness of the intrusion software language threatens to do more to hinder better security than help it.

A second major risk lies in the propensity of export controls to push transfers to black markets. In doing so, defensive actors lose important visibility into the market for offensive products, thereby hindering their ability to forecast and proactively defend.

The current feasibility of export controls to meaningfully decrease the spread of offensive cyber capability is limited. However, in order to further explore the potential feasibility of an export controls intervention policymakers should work to better understand the two major risks in order to manage them as well as working to address the three major challenges regarding thresholds, verification, and punishment.

TOOLS FOR STATES OR LIKE-MINDED ACTORS

In addition to sweeping international agreements, states have tools that they could leverage unilaterally or within like-minded coalitions.

Table 16: Summary Tools for States or Like-minded Actors

	TrACE Framework Element Addressed	Actor Effected	Current Feasibility	Longue Durée
Manipulate the market through purchasing power	Transfer and Capabilities	Developers, Deployers, and Enablers	Low	Yes
Enhance defensive capabilities	Capabilities and Effects	Defenders, Deployers	High	Yes
Enhance offensive capabilities (cyber and non-cyber)	Capabilities and Effects	Deployers	High	Yes
Diplomatic toolbox	Actors and Effects	Deployers	High	Yes

Market Manipulations

Given that there is a market for cyber capabilities, however fragmented across language and skill level, how can market manipulation contribute to a counter-proliferation strategy? There are at least three basic strategies to manipulate a market with as many information asymmetries as that for cyber capabilities - undermine trust, affect supply or demand,

[200] Cheri McGuire, "U.S. Commerce Department Controversial Cybersecurity Rule Will Weaken Security Industry and Worldwide Protections," *Symantec Global Government Affairs* (blog), accessed November 11, 2017, http://www.symantec.com/connect/blogs/us-commerce-department-controversial-cybersecurity-rule-will-weaken-security-industry-and-worl.

or break market functionality. The last is the most straightforward - block markets to make them inaccessible to buyers or disrupt the market for transaction critical services like payment processing or hosting.[201]

Disrupting supply or demand require more influence on the underlying goods at trade. One proposal, from Dan Geer in his now famous 2014 keynote for the BlackHat conference, suggested that the United States could allocate the resources necessary to buy up all software vulnerabilities.[202] Accepting that the speech was intended to kickstart a conversation about software liability, the proposal was nonetheless both provocative and compelling. The idea that one player in the market could vacuum up the available supply to such an extent that new sales would be possible only on the fringes, would limit new capabilities to those groups who could develop them, or obtain them directly from a developer.

An alternative to Geer's approach would be to enhance the speed and depth of vulnerability discovery and patching states could undermine the development of cyber capabilities which rely on software vulnerabilities by encouraging more effective vulnerability discovery, disclosure, and patching. Reducing the supply of vulnerabilities through this discovery and patching will raise of the cost of acquiring these capabilities and help disrupt the activity of sellers unable to update their products fast enough. This market manipulation doesn't involve purchasing vulnerabilities directly, instead it reduce their useful life by more rapidly patching them.

Not all vulnerabilities are equally easy to find or take advantage of and not all offensive capabilities require the use of one of these vulnerabilities. This proposal to target vulnerabilities for discovery, disclosure, and patching targets only those offensive capabilities which take advantage of these software flaws. This is not an argument for how to restrict the transfer of offensive capabilities more effectively. Instead, it is a means of focusing on a common supporting component for many offensive cyber capabilities.

Disrupting trust is a more amorphous set of objectives. The seizure of Alphabay followed a period where the site was operated by law enforcement, leading to the possibility that every future market going dark could be accompanied by the same long tail. Breeding this sort of suspicion is one thing with these underground markets but is more difficult looking at many of the companies involved in selling capabilities in whole or in part like Zerodium, Hacking Team, or NSO Group. The use of legal discovery mechanisms to force client lists and other sales documents from these groups into the public domain could be a means to create mistrust or the potential for compromise in the minds of secrecy minded customers.

ENHANCE OFFENSIVE AND DEFENSIVE CAPABILITY

A growing number of states have already stated that they are looking to increase offensive capability. However, it is just as important to focus on the defensive side. In this case, the nuclear analogy is a missile defense system, designed to make it more difficult to achieve the effect of nuclear capability once developed or purchased. In addition to ultimately diminishing the effects of proliferation, rendering capability less or unuseful is also likely to dampen the demand for offensive capability. Diminishing the attack surface, through interventions in the market for vulnerabilities like the one described above, is one way to diminish utility. An increased velocity of vulnerability discovery and reporting renders capabilities built on those vulnerabilities transient, diminishing their long-term utility.

[201] https://motherboard.vice.com/en_us/article/evd7xw/us-europol-and-netherlands-announce-shutdowns-of-two-massive-dark-web-markets and http://www.tandfonline.com/doi/full/10.1080/17440572.2016.1197123

[202] https://www.darkreading.com/dan-geer-touts-liability-policies-for-software-vulnerabilities/d/d-id/1297838?piddl_msgorder=thrd

However, more can still be done to diminish the utility of offensive cyber capabilities including two goals achievable in the near term. First is enhancing the speed and volume of information sharing between organizations to more rapidly counter attacker innovation and changes in capabilities. Attackers will become more conservative in target selection and capability deployment if any target they assault can alert all others to the details of their attack. Second is an emphasis on cloud computing, where defensive organizations can implement changes and patch vulnerabilities for all users in an organization much more rapidly than in the traditional enterprise computing model. These approaches are technical but can be encouraged by international agreement (especially information sharing) and or soft norms like the adoption of principles through plurilateral forums, like the OSCE or ASEAN, which encourage regulatory environments and security cooperation which complement these approaches.

DIPLOMATIC TOOLBOX

In addition to activities designed to address the proliferation of offensive cyber capability, states and other actors can work to diminish the utility of capability, once spread. Diplomatic efforts, like the European Union's Diplomatic Toolbox to deter cyberattacks are a key way to do this, and sanctions are at the heart of diplomatic efforts and conceived to be the key tool for deterring, compelling, and/or incapacitating adversaries.[203]

Sanctions are a key tool to punish an actor for bad behavior. When utilized after an incident, sanctions are intended raise the perceived cost of an action to an adversary, thereby deterring further, similar action. However, sanctions can also be utilized before adversarial action takes place as capability is being developed. This kind of preemptive punishment is designed to disincentivize future action.

A second potential use for sanctions lies in incapacitating adversaries with limited resources. Because the development of some strata of capability (and perhaps more importantly the persistent development and deployment of some strata) requires institutional strength and financial backing, targeted sanctions could diminish the capacity of a *developer* to produce capability. Targeted sanctions can also provide a powerful disincentive for individuals contributing to development on their own or as part of a team. Additionally, sanctions could diminish the capacity of some *deployers* to purchase capability.

Most impactful when they are implemented universally, sanctions pose substantial risk of collateral harms and can be politically fraught for fragile alliances or coalitions of consensus. Other challenges associated with a sanctions regime to address the *transfer* and *actors* in the proliferation ecosystem are numerous. One key challenge lies in identifying key individuals or groups of both *developers* and *deployers*. Furthermore, sanctions are likely to only have an appreciable impact on *actors* with limited resources.

[203] Sico van der Meer - "EU Creates a Diplomatic Toolbox to Deter Cyberattacks," Council on Foreign Relations - Net Politics Blog, June 20, 2017, https://www.cfr.org/blog/eu-creates-diplomatic-toolbox-deter-cyberattacks.

SECTION 6: RECOMMENDATIONS

In this section, we first explain the need for patience, then provide a series of recommendations aimed at: (1) increasing the cost of developing offensive cyber capabilities, (2) diminishing the utility of capability once spread, and (3) further exploring ways to increase barriers to spreading offensive cyber capability. The TrACE framework provides a good guide for researchers and policy-makers for conceptualizing proliferation of capability, but more work is needed to truly understand the mechanics of development, spread, and deployment.

1. PATIENCE.

The first lesson that policy-makers must heed is that the construction of a security regime—and particularly of a counterproliferation regime—is arduous. It takes time, subject matter expertise needs to be developed and infused into policy circles, hurdles like crafting a viable verification or inspection mechanisms must eventually be overcome, and an understanding of the above and below ground markets for relevant goods and services must be developed and leveraged. Efforts like the preparatory workshops for the Group of Governmental Experts (GGE) meetings and indeed the Global Commission on the Stability of CyberSpace (GCSC) aid in that essential diffusion of expertise.

For the policy-makers involved in the process, patience is paramount. In his 1953 "Atoms for Peace" speech, Eisenhower noted the imperativeness of patience, saying:

> *"In this quest, I know that we must not lack patience. I know that in a world divided, such as ours today, salvation cannot be attained by one dramatic act..."*[204] Eisenhower's words ring equally true today in the context of cybersecurity.

As we've witnessed in the past, negotiation processes around these sorts of regimes are generally long, drawn-out, and controversial. The NPT took nearly 20 years to craft from its early beginnings in 1957 to end and nations continued to iterate on the overarching regime until the mid-1990s with the Comprehensive Nuclear-Test Ban Treaty. Similarly, negotiating the surprise inspection provision of the CWC during the tensions of the Cold War was incredibly difficult diplomatically, but ultimately fruitful.

Policy-makers must also accept that the process of building a regime will not be easy. As demonstrated by the shortcomings of the Wassenaar Arrangement, it is possible that the international community will not be able to simply transpose an existing model on top of the cybersecurity problem. Instead, it is far more likely that new and innovative models will need to be built to address the challenge. In order to craft a regime that both has the desired effect and minimizes the negative externalities, a deep understanding of the technologies in question must be infused into the policy process. Practicing physicists made the progress of the NPT, from hard initial negotiations to eventual ratification, possible. While the cybersecurity threat may not be existential, as the nuclear threat, the risks should not be ignored.

[204] Eisenhower, Atoms for Peace.

2. INCREASE THE COST OF DEVELOPING OFFENSIVE CYBER CAPABILITIES

Raising the cost of offensive cyber capabilities can be accomplished through reducing the supply (and thus cost) of software vulnerabilities and increasing the speed at which defenders can adapt to attackers by enhancing the use of cloud computing. By raising the cost of development, the number of developers in the market will decrease. This supply-side decrease could then reverberate throughout the proliferation ecosystem, limiting the transfer, diminishing the number of deployers, and possibly limiting capability to primarily the most profitable forms of capability.

Reducing the supply of vulnerabilities will raise the cost of acquiring offensive cyber capabilities and help disrupt the activity of actors involved in transferring capabilities to others by forcing them to update their products with unsustainable rapidity. This strategy to counter proliferation in cyberspace could encourage more effective discovery, disclosure, and patching of software bug instead of building new or more refined export controls. It could enhance information sharing between state organizations with insight into attacker trends and major software vendors and cloud service providers. Reducing the utility of cyber capabilities looks to attack demand rather than use of these capabilities, with benefits that will trickle up to the larger security ecosystem.[205]

Key to limiting the use of malware is modifying attacker's incentives to build and deploy this software. This can be accomplished by increasing the pace and volume of software vulnerability discovery, disclosure, patch development, and patch application. The result of these changes would undermine the supply of software vulnerabilities available to attackers using malware which depend on these vulnerabilities. This would reduce how long any piece of malware might be useful for, before its targets had patched their software. Malware authors would have to write code faster and faster to keep it current, increasing costs and potentially driving many out of the business altogether. This accelerated vulnerability disclosure and patching cycle would also lead to more robust software, making it easier to defend organizations, though it may adversely affect a country's own offensive arsenal.

The resulting increase in costs to develop offensive cyber capabilities target attackers' incentives—pricing less-resourced actors out of the security ecosystem and constraining the capabilities of better resourced groups. This pushes states towards collaboration with the private sector to influence attacker behavior by shifting the incentives to develop and use capabilities. As such it implicates both actors and capabilities in the TrACE model, looking at a public-private nexus.

Offensive cyber capabilities often depends on exploits targeting vulnerabilities in software or hardware to gain and maintain access to computer systems, with destructive attacks like Stuxnet espionage operations like Red October, even common surveillance tools.[206] Most cyber capabilities requires these vulnerabilities at some stage of operation

[205] Trey Herr, "Countering the Proliferation of Malware: Targeting the Vulnerability Lifecycle," Belfer Center White Paper, Cyber Security Project Paper (Cambridge, MA: Harvard Kennedy School, June 27, 2017).

[206] Stuxnet - Nicolas Falliere, Liam O. Murchu, and Eric Chien, "W32. Stuxnet Dossier" (Symantec, 2011), http://www.h4ckr.us/library/Documents/ICS_Events/Stuxnet%20Dossier%20(Symantec)%20v1.4.pdf; Ralph Langner, "Langner - To Kill a Centrifuge.pdf" (The Langner Group, November 2013), http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.

Red October - Kaspersky, "'Red October'. Detailed Malware Description," *Securelist.com*, January 17, 2013, http://www.securelist.com/en/analysis/204792265/Red_October_Detailed_Malware_Description_1_First_Stage_of_Attack#1.

Surveillance tools - Bill Marczak and John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used against a UAE Human Rights Defender," *The Citizen Lab*, August 24, 2016, https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/; Stefan Esser, "PEGASUS iOS Kernel Vulnerability Explained |

but not all. Reducing the supply of these vulnerabilities would limit those available to attackers and increase the cost necessary to acquire them. Groups with few resources might avoid targets while less cost-sensitive organizations, like major intelligence agencies, may find themselves constrained by this shortfall in new exploits to enable their operation. Limiting the supply of vulnerabilities doesn't remove attackers from the security ecosystem but it disrupts the process of developing and deploying malware, making these critical pieces of information scarce and thus more difficult to acquire. Versions of this approach have already had success with lower hanging fruit, as more secure web application technologies have impacted the supply of vulnerabilities for commonly used exploit kits.[207]

Counter-proliferation can also raise the cost to attackers by making defenders more agile and quick to adapt through expanded adoption of cloud computing. Cloud computing enables vendors and defensive organizations to more rapidly shift defensive technologies to blunt attacker's innovations, for example by making global changes to an organization's entire software stack in a few short minutes. The size of some global cloud providers also means they can see even small and highly targeted attacks, rapidly disseminating information about the threat to defend organizations around the world. This increases the likelihood that an offensive capability, technique, or tactic, once used, will be exposed and its value commensurately reduced.

3. FURTHER EXPLORE WAYS TO INCREASE BARRIERS TO SPREADING OFFENSIVE CYBER CAPABILITY

There has been a lively debate over the potential utility of agreements to limit the spread of offensive capabilities, potentially along the line of arms control agreements for nuclear and biological weapons. This topic is one that deserves further development and study as a standalone topic outside the specific discussion of counterproliferation. As such, we note it here but leave it as a starting point for further exploration.

Defining offensive capabilities in relation to effect is likely to become a prominent part of the next phase of debate over proliferation. This Commission could convene expert working groups to set tiers, or thresholds, between different types of capabilities according to the severity of effects they produce. Non-destructive capabilities, taken at sufficient scale like botnets, or at important points in a process, like information on an industrial control system, can impose substantial harm. Developing a threshold for determining what effects are significant however remains a largely political act in its explicit valuation of some potential targets over others. For this reason, we believe the conversation over these thresholds should start within the policy community and this Commission rather than this document.

The policy community should explore the applicability of all models focused on the spread of goods, materials, information, and more. While many will be drawn to nuclear comparisons—possibly simply due to language parallels involving the word "proliferation"—explorations should not be so limited.

SektionEins GmbH," September 2, 2016, http://sektioneins.de/en/blog/16-09-02-pegasus-ios-kernel-vulnerability-explained.html.

[207] https://www.trustwave.com/Resources/Trustwave-Blog/Why-Exploit-Kits-Are-Going-Dark/

CONCLUSIONS

The core of this report, the TrACE framework, is intended as an evergreen model to provide policymakers and others looking at proliferation within cybersecurity a means to conceptualize and discuss major factors in proliferation. In our development of this framework, we offer a snapshot of the security ecosystem and proliferation activities as they can be observed at this moment.

Key to understanding proliferation with an aim towards countering it is differentiating between types of capabilities. We know that not all capability is created equally. The development of Stuxnet, for example, is rumored to have cost orders of magnitude more than the development of simple phishing tools to steal credentials. Intuition tells us that the more resource-intensive capabilities are likely the ripest targets for counterproliferation efforts.

Thus, a key element for consideration by analysts and researchers is how to set these tiers or thresholds to differentiate types of capabilities. Conventional analysis tends to conflate effects with capabilities but this undersells the disparity with regard to ease of development between some capabilities that cause similar effects. We suggest that the development of such thresholds requires careful consideration from the policy and technical community and would be a meaningful step towards understanding the proliferation ecosystem, but falls outside the scope of this document.

To that end, this exploration is simply a starting point to prod the international conversation about cybersecurity in what we view to be a more meaningful direction. However, this report does not portend to have all the answers, and it may indeed offer more questions that it does answers. To help guide future research and exploration, we outline a set of those open questions here:

- What are the best forums for counterproliferation discussions internationally? Does counterproliferation lend itself to an approach embracing only like-minded participants or is it feasible in a broader multi-lateral format?
- In the context of cyber proliferation, what sorts of scenarios are the international community most concerned about? Would the mechanics of slowing or blocking the proliferation of capability to non-state terror groups like the Islamic State differ from countering the proliferation of capability to a large nation-state adversary?
- What is the threshold on capabilities a state could transfer to a malicious actor to violate a consensus or normative limit?
- While we offer an exploration of potential export and arms control approaches, what other international mechanisms might produce positive results, and what models might we explore to help generate better understanding about countering the spread of goods, services, information, and more? What might we learn about the spread of offensive cyber capability from experiences in the chemical and biological weapons community? What about from unmanned aerial vehicles? Are there lessons to be drawn from experiences in countering narcotics or disease control? What other areas are ripe for exploration?

The immediate and increasing threat of cyber capabilities may drive an inclination on the part of policymakers around the world to act swiftly and decisively to counter the proliferation of these capabilities. However, without the requisite knowledge about how the proliferation ecosystem functions, how capability is developed and spreads, and a clear picture of what mechanisms might be available to slow, block, or otherwise counter this proliferation, hasty policy interventions are likely to fail—or worse: throw further fuel on the problem.