Civilians in Cyberspace: A New Line of Defense

Jessica Draper
Peace Research Institute
Internship Paper
Dr. Niklas Schörnig
January 15, 2020

CONTENTS

FIGURES

TABLES

INTRODUCTION

As cyber attacks and related threats continue to make headlines, a lively debate has emerged among scholars regarding the feasibility of cyber deterrence. While some argue traditional deterrence theories can be adjusted for and applied to the cyber domain, others strongly advocate a complete rethinking of cyber deterrence that incorporates more nuance and flexibility. Meanwhile, states are rapidly introducing their national cyber defense strategies. Some nations have experienced the costs of cyber attacks more than others, but all states seem to understand the need to develop a national strategy against malicious cyber activity. The question is, are states capturing every tool at their disposal in these strategies for both cyber deterrence and defense?

In contrast to conventional war and conflict, the cyber domain presents unique characteristics that fundamentally reshape how – and by whom – war is fought. The battlefield is no longer limited to a geographic area with opposing armies on either side; neither is it limited to villages and cities located in armed conflict zones. Every device connected to a network, regardless of nation or region, is a potential target. This has created a situation where billions of individuals who work with or own such devices are operating in a battle zone whether they are aware of it or not.

While terms such as "cyber war" and "cyber battlefields" are ill-defined and may be more hyperbole than reality, the fact remains that interstate conflict has moved into cyber territory where billions of civilians could be unknowing participants. The open nature of the internet means that states with ill-intent and ordinary citizens worldwide are coexisting in the same digital plane. In no other interstate conflict context has this been the case.

Scholars discussing cyber deterrence and defense often refer to the important role of overt offensive cyber capabilities and strong, resilient networks (Crosston 2011; Libicki 2018; Wilner 2017). As in conventional deterrence theory, the focus of cyber deterrence tends to rely heavily on technological capabilities. Rarely is the human user mentioned when considering cyber vulnerabilities and potential deterrence strategy. In a 2014 report, IBM reported human error as a contributing factor in over 90% of cyber incidents (IBM Global Technology Services 2014). Seven of ten high-profile cyber attacks examined by Kadivar (2014) started with phishing or spear phishing, methods which rely on deceiving vulnerable users. Regardless of strong technological cyber capabilities, attackers can still gain unauthorized entry with relative ease by simply exploiting human weaknesses. There is a strong argument to be made that states ought to consider such human vulnerabilities

when developing their national cyber strategies. This paper investigates if and to what extent states are doing just that.

Before investigating whether states are including user-centered approaches in their strategies, this analysis first provides a brief yet comprehensive overview of the central objects of discussion. Defining "cyber attacks," discussing deterrence theory, and summarizing the current debate on cyber deterrence offers important context. The next section explores the efforts and outcomes of national cyber strategy development over the years in response to rising cyber threats. The central argument in favor of user-tailored approaches to cyber deterrence and defense is then presented, followed by an analysis of existing national strategies and how they address the role of users with regard to cybersecurity. The paper concludes with a discussion of the analysis and final remarks.

SETTING THE STAGE

Defining "Cyber Attacks"

Cyber attacks. Cyber operations. Cyber incidents. These terms are often used interchangeably by scholars, practitioners, and the public alike when referring to a range of malicious activity occurring in cyberspace. As a still-emerging modern phenomena, it is not surprising a standardized vocabulary has not yet been developed to define such activities.

While the ambiguity and non-standardization of these terms has been acknowledged by some (Owens, Dam, and Lin 2009; Hathaway et al. 2012; Kadivar 2014), much of the literature on cyber deterrence and defense remains terminologically imprecise. Most papers on the subject fail to define what is meant by "cyber attack" or "cyber operations" and simply offer a few observable examples instead. Real-world examples are extremely useful; however, without clearly establishing what is being referred to or discussed, ambiguity around these terms and phenomena will continue. As Hathaway et al. (2012) alludes to in a legal context, ill-defined digital security threats makes drafting appropriate responses all the more difficult. The focus of this section is not to propose the be-all and end-all terminology for malicious cyber behavior. The focus is to provide an overview of concepts and clarify the terms in use in the present paper.

According to the U.S. Department of Defense, cyber*space* is a "global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (Theohary 2018,

1). In simpler words, Singer and Friedman (2013) describe it as "the realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online" (13). It is an information environment consisting of digital, physical, and cognitive structures which are constantly evolving with each passing year (Singer and Friedman 2013).

Activity that occurs via computer networks, then, is occurring in cyberspace. Behaviors in cyberspace can vary in intent and purpose, just as they do in physical spaces. "Malicious cyber activity" refers to any behaviour in cyberspace that *intends* to be malicious against some target. However, as the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) points out, there is no internationally agreed upon definition for the term "cyber attack" (CCDCOE 2013) as countries differ in how they choose to understand and define behaviors that constitute an "attack." In an effort to clarify terms and find common international agreement from a legal perspective, Hathaway et al. (2012) recommends the following definition for a cyber attack:

A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose. (826)

In explaining the reasoning behind each component of this definition, a number of debates reveal themselves. Hathway et al. (2012) suggests a definition where a) the action itself does not necessarily have to occur in cyberspace (i.e. a regular kinetic explosive that severs a network could be considered a cyber attack); b) an action merely stealing information or observing a network in a way that does not affect its *function* is not considered a cyber attack (rather, cyber espionage)[1]; c) the political or national security purpose of the cyber attack distinguishes it from cyber crime; and d) the attacker must not necessarily be a nation-state.

Despite the effort towards establishing a common conception, these four elements are frequently challenged in practice. For example, Germany's definition of a cyber attack understands the attack as occurring in cyberspace, includes non-function-altering attacks (e.g. theft of confidential information), and does not specify a political or national security purpose (Federal Ministry of the Interior 2011). Additionally, some scholars and data collectors choose to limit cyber attacks to only those that are carried out (or sponsored) by the state (Osawa 2017; Council of Foreign Relations, n.d.; Maness, Valeriano, and

1. It is important to note that some experts, such as Thomas Rheinhold from Wissenschaft und Technik für Frieden und Sicherheit (PEASEC), argue that even such "passive" behaviors such as copying and transferring data still technically affects certain functions and pose potential dangers to the system.

Jensen 2019). Apart from these debates, there are also some who view coordinated disinformation campaigns as well-within the scope of a cyber attack (Osawa 2017). The line differentiating "malicious cyber activity" and a "cyber attack" is, therefore, very unclear.

It is likely this very reason why some choose to avoid the term "cyber attack" altogether. In their book, *Cyber Strategy: The Evolving Character of Power and Coercion*, Valeriano, Jensen, and Maness (2018) consistently use "cyber strategy" and "cyber operations" when referring to actions such as website defacement, the stealing and manipulation of information, or the destruction or disabling of networks and critical infrastructure systems. They categorize various malicious cyber activities into four types: vandalism, denial of service, network intrusion, and network infiltration (Maness, Valeriano, and Jensen 2019). In a similar manner, the Council on Foreign Relations uses terms such as "cyber operations" and "cyber incidents" in their Cyber Operations Tracker, a database of publicly known state-sponsored incidents (Council of Foreign Relations, n.d.).

To avoid the debates that come along with the use of "cyber attack," I will opt to use the terms "cyber incident" and "cyber operation" as well. In doing so, I refer to actions "initiated in cyberspace to cause harm by compromising communications, information, or other systems, or the information that is stored, processed, or transmitted in these systems" (CCDCOE 2013). This definition includes a range of activities, including those outlined in the Dyadic Cyber Incident and Dispute Dataset codebook (Maness, Valeriano, and Jensen 2019, see table 1). This definition does not include disinformation (i.e. "fake news") campaigns.

While legal and normative discussions around the term "cyber attack" continue, having this broad definition of malicious cyber activity in mind when considering defense and deterrence offers a number of benefits. It allows scholars and practitioners to "think big" about existing and future cyber threats. Addressing only a subset of a subset of cyber incidents in national defense and deterrence strategies is neither practical nor useful. While one size certainly won't fit all, solutions must take the full picture into account.

Deterrence Theory

The literature on classical deterrence theory is vast and will not be covered in full in this section. Rather, I will briefly discuss the concept of deterrence and differentiate between deterrence by punishment and deterrence by denial.

In his eloquent summary on deterrence theory, Wilner (2017) highlights four important assumptions. First, "deterrence prompts voluntary changes in behavior" (310). Deterrence is a choice made by one's adversary; it does not entail brute force or incapacitation. Second, the adversaries must be rational actors. Deterring an enemy from an attack only

Incident Method	Description
Vandalism	Website defacement or destruction
Distributed Denial of Service	DDoS attacks flood particular Internet sites, servers, or routers with more requests for data than the site can respond to or process. The effect of such an attack effectively shuts down the site thus preventing access or usage.
Network Intrusion	Trapdoors or Trojans are unauthorized software added to a program to allow entry into a victim's network or software program to permit future access to a site once it has been initially attacked. The purpose of trapdoors is to steal sensitive information from secured sites. Spear phishing is utilized to inject these cyber methods into networks. Here the initiator sends emails to employees or contractors of the targeted network, and if the email is opened, the intrusion is introduced to the system. The botnet technique is another option where a human being injects the intrusion from a portable drive such as a USB or disk.
Network Infiltration	Examples of attacks include logic bombs, viruses, packet sniffers, and keystroke logging. These methods force computers or networks to undertake tasks that they would normally not undertake.

Table 1: Cyber Incident Methods from DCID codebook (Maness, Valeriano, and Jensen 2019)

works when the enemy is able to calculate costs and benefits and respond accordingly. Third, deterrence involves at least two actors whereby the defender defines "unwanted behaviors to the challenger, and communicate[s] or signal[s] a willingness to punish violations...Red lines must be drawn, communicated, and defended" (310). This point is a critical component of deterrence; in order for the challenger to make an accurate cost-benefit analysis, it must have the impetus to do so. Fourth, deterrence is generally only effective against a known (or suspected) adversary. Threats are strongest against a clear target; threats against an ambiguous adversary "may miss their mark" and debilitate the deterrence strategy altogether (310). In sum, Wilner (2017) offers the following description:

> Deterrence rests on convincing an adversary that the costs of taking a particular action outweigh the potential benefits. Deterrence is fundamentally about manipulating another's behavior in ways that suit your own goals. It is about influencing what economists call the cost-benefit calculus of decision making. (310)

Costs and benefits form the foundation of deterrence theory. Given that adversaries are rational, it is through this calculation that deterrence works or not. The only calculation that results in effective deterrence is one where the costs to the adversary outweigh the benefits. How does an actor administer such costs, then?

The most obvious response is retaliation, i.e. a "second-strike" capability. The idea is if an adversary chooses to attack, they will experience a counterattack that is so costly they would be better off having not attacked in the first place. By this logical calculation, they are, thus, deterred from conducting the initial attack. This idea is captured in the doctrine of Mutually Assured Destruction, or MAD, regarding nuclear deterrence during the Cold War. If the USSR were to launch a nuclear strike against the US, the US has the technological capability to immediately strike back (i.e. "second-strike"), resulting in mutually assured destruction for both powers, thus deterring the USSR's initial strike.

While nuclear retaliation is an obvious example, it works through other means, as well. As Wilner (2017) points out, "actors can use a combination of threats, like conventional or nuclear attack, military intervention, economic sanctions, and diplomatic pressure to shape an adversary's behavior" (310). That is, to increase the costs for a challenger with the aim of deterrence.

Increasing the costs in such a retaliatory-like manner is often referred to as deterrence by punishment. However, it is also possible to manipulate the "benefits" variable of the equation. Instead of raising the costs, an actor can seek to deny the adversary the benefits it hopes to achieve by an attack. This strategy is referred to as deterrence by denial.

Deterrence by denial can be achieved through simply strengthening defense (i.e. higher castle walls). While defense and deterrence are two separate concepts, they inform each, thus making them fairly intertwined. If a successful attack becomes more difficult to achieve due to strong defenses, it restricts the benefits (and potentially increases costs) to the adversary, ideally resulting in a deterred attack. Additionally, deterrence by denial can be achieved through resilience. "Resilience is the ability to bounce back, to mitigate the effects of an attack, to recover quickly after getting hit...[and] robs would-be aggressors of their objectives and strategic success" (Wilner 2017, 310). While conducting the attack may be possible, the likelihood of success drops dramatically when defenders are resilient and can withstand such attacks with minimal damage. So long as the resilience factor is communicated to and deemed credible by the adversary, it subtracts from the benefits and, in turn, deters the initial attack.

In both deterrence by punishment and deterrence by denial, the four main features highlighted by Wilner (Wilner 2017) must be present in order for either to be effective

(choice, rational actors, communication, clear target). These deterrence strategies can be (and are) applied in a variety of scenarios at numerous levels of power. In a national security context, states are motivated to increase both offensive and defensive capabilities for this very reason. Offensive capabilities aid deterrence by punishment while defensive capabilities aid deterrence by denial. While these concepts build the basis of classical deterrence theory, how might they operate in practice in the cyber domain?

Challenges of Cyber Deterrence

In thinking about deterrence strategy within the realm of cyberspace, there is disagreement in the literature about the best approach. While some favor a deterrence by punishment approach (Crosston 2011; Libicki 2018), others argue deterrence by denial is the most feasible (Iasiello 2013; Schulze 2019). Departing from either strategy, some say deterrence may not even be possible (Geers 2010) and others say more comprehensive and nuanced approaches are necessary (Wilner 2017; Lindsay 2015; Buchanan 2014; Tor 2017; Harknett, Callaghan, and Kauffman 2010). There is no clear consensus in how best to deter adversarial offensive cyber operations. We are only now beginning to fully understand the threats that are emerging and the technological capabilities required to face them. This section will focus on the unique characteristics of cyberspace and cyber incidents that make deterrence especially complicated.

The literature points to at least six challenges that deterrence efforts face in the cyber domain: the attribution problem, irrational actors, types of attacks, lack of norms, proportionality, and uncertainty. Authors may disagree how and to what extent these challenges prevent effective deterrence, but they are all identified as deterrence obstacles.

The first challenge has been frequently discussed by scholars, practitioners, and technicians: the attribution problem. When a cyber incident occurs, it can be extremely difficult, perhaps impossible, to accurately detect who is behind the operation. This limitation, as some argue, makes it exceedingly difficult to retaliate. Knowing that the anonymity of such incidents protects against retaliation, perpetrators are not deterred from engaging in such behaviors in the first place. Thus, the anonymous-enabling nature of cyberspace weakens the capabilities of a robust deterrence mechanism, especially via deterrence by punishment (Geers 2010; Iasiello 2013; Wilner 2017; Crosston 2011).

However, while noting the challenges posed by the attribution problem, some argue that this does not completely hinder deterrence strategy. Crosston (2011) suggests an open, transparent, and offensive "cyber-MAD" strategy that does not necessarily depend on attribution to be effective:

> While this article testifies to the problem of attribution, this does not lead to an argument for moving away from old models of retaliatory deterrence but actually the reverse: a retaliatory cyber model would not be about who to launch missiles against, but rather enforcing the perception of massive technological/ infrastructural debilitation if even the suspicion of an attack is determined and attributed. Nuclear MAD was successful not because various states actually launched nuclear weapons; it succeeded because of the conviction across all parties that an attack of this nature would be so universally destructive that the cost far outweighed any poten- tial benefits. A cyber-MAD model has to operate on this same principle, only with virtual weapons rather than kinetic ones. (111)

While attribution certainly helps, Crosston's deterrence strategy rests more in perception of transparent offensive capabilities than actual retaliatory attacks against particular actors. Kugler (2011) also argues that the attribution problem is not as restrictive as others may view it. "Although attribution will remain a serious problem, the fear that the attribution problem wholly cripples any hope of detection and deterrence is misplaced" (Kugler 2011, 317). He argues that, in certain strategic contexts, attackers in cyberspace will be willing to identity themselves or, alternatively, their identities can be reliably inferred (Kugler 2011, 310).

This brings us to a second major challenge of cyber deterrence: the irrationality of certain actors. While nation-states may generally act rationally in their cost-benefit calculations, many point out the threat of actors who do not make such rational calculations such as terrorists, hacktivist organizations, or other "cyber misfits and miscreants" (Iasiello 2013; Wilner 2017, 313). As Iasiello (2013) summarizes clearly, "if the adversary does not hold a rational view of the world and his place in it, or he does not have anything to lose or be threatened, he may be very difficult to deter from a specific course of action" (46). While deterrence against nation-states may generally hold, the low-cost of entry into an aggressive cyber domain means there will undoubtedly be actors less responsive to deterrence strategies. Kugler argues, however, that "rationality" is a relative term and virtually all actors, nonstate actors included, are governed by "explicit motives, goals, and awareness of costs and risks" (325-326). This view suggests that deterrence strategies simply ought to be more creative and nuanced in how they build their deterrence mechanisms against such actors – as Kugler calls it, a "tailored" approach (2011).

A third major challenge of cyber deterrence is the sheer variety of malicious activities and behaviors that can be conducted in cyberspace. As illustrated earlier in table 1, there are different types of operations that may require different responses. It could be the case that a network intrusion or infiltration is not even noticed until months after the fact. As deterrence by denial has already failed in such a case, deterrence by punishment

is heavily debilitated when defenders are not aware they have something to retaliate against (Wilner 2017). Additionally, how one deters low-level incidents (if at all) will be drastically different from how one deters against more severe attacks. States may further make an important distinction between legitimate espionage and statecraft versus an unlawful "attack" or incident that requires some response. The literature identifies the diversity of cyber operations as an obstacle for cyber deterrence, but argues that it can be overcome with a dynamic, nuanced strategy (Wilner 2017; Buchanan 2014; Kugler 2011).

The lack of widely-accepted norms of behavior in cyberspace is a fourth challenge in cyber deterrence. If a common set of norms and standards are agreed upon, especially by allies in a context of collective security (e.g. NATO), then violators of such norms may be deterred by the threat of collective defense (Osawa 2017). However, without a "consensus for operating norms of behavior in cyberspace," communicating desired behaviors and red lines becomes more difficult, a task that is critical for an effective deterrence strategy. Communication based on a common language and understanding is especially important in the developing cyber domain; unfortunately, such norms are still in flux. (Iasiello 2013).

Other issues such as proportionality and uncertainty also pose additional challenges for cyber deterrence. Determining a proportional response to an aggressive cyber operation is difficult in practice, particularly due to the uncertainty of cyber effects (Geers 2010; Iasiello 2013; Crosston 2011; Harknett, Callaghan, and Kauffman 2010; Libicki 2018). For example, Geers (2010) points to the example of "a misfire in cyberspace [that] might adversely affect critical national infrastructure such as a hospital, which could result in a violation of the Geneva Convention" (301). These challenges weaken credibility and therefore weaken deterrence effectiveness.

In considering these challenges that are rather unique to the cyber domain, disagreements continue as to how a deterrence strategy might overcome these challenges, if even possible. They appear to be particularly tricky for deterrence by punishment methods. This is why a deterrence by denial approach or, alternatively, a more tailored, nuanced approach, is often argued to be more feasible over retaliatory cyber operations (Iasiello 2013; Schulze 2019; Kugler 2011; Wilner 2017; Buchanan 2014).

DEVELOPING A NATIONAL CYBER STRATEGY

National Strategies in Response to Cyber Incidents and Threats

The threat of malicious cyber operations is a strictly modern one. While the internet has technically existed since at least the 1970s, the threat of conflict within cyberspace, particularly between states, only begun in 2007 with the first known state-sponsored cyber operation (Wilner 2017):

> In the Estonian case, a nationalistic confrontation between Russia and Estonia over the removal of a Bronze Soviet Red Army Soldier symbolizing Soviet oppression triggered large scale distributed denial-of-service (DDoS) cyberattacks targeting the country's infrastructure, causing a shutdown of the websites of government authorities, political parties, and institutions in the financial sector. At that time Estonia depended heavily on information technology and was one of the countries with the most advanced information infrastructure in Europe, so that the attack was quite successful. In the second wave of DDoS attacks on May 10, 2007, nearly one million computers abroad requested Estonian servers to respond to external communications and filled the network of Estonia with meaningless packets. As a result, online banking services and ATMs of Estonia's two big banks came to a standstill. (115)

As information and communication technologies (ICT) develop and become further integrated into state functions, the threat of malicious cyber operations becomes more serious. The growing global dependence on the internet and digital technologies "makes a country and society more vulnerable to cyberattack" (Osawa 2017, 114). As illustrated by the Estonia case in 2007, their advanced ICT capabilities made them more vulnerable to Russian cyber operations.

ICT coverage around the world only grows each year (International Telecommunication Union 2019), making such vulnerabilities a cause for concern for an increasing number of countries. Data from both the Dyadic Cyber Incident and Dispute Dataset (DCID) and the Council on Foreign Relations show that the world is experiencing a rising level of cyber incidents (see figure 1). As more states develop their ICT capabilities, they expose themselves to increased risk.

International efforts to establish common laws and norms regarding offensive cyber behavior between states have certainly occurred in the last decade in response to these threats. For example, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, both in 2013 and 2015, agreed that international law (such as the UN Charter) ought to regulate such activities and further recommended that "states cooperate to prevent harmful ICT

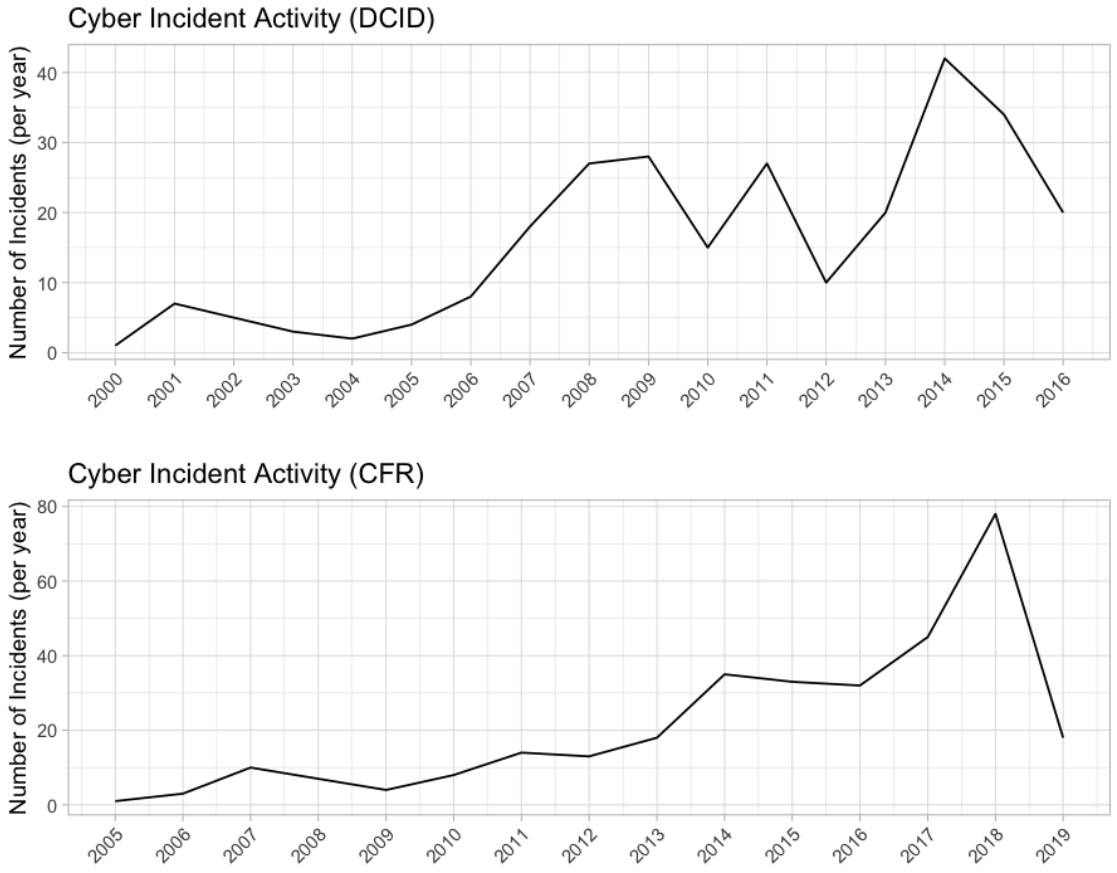

Figure 1: Cyber incidents per year over time from DCID source and CFR source, 2000-2019 (Maness, Valeriano, and Jensen 2019; Council of Foreign Relations, n.d.)

practices and should not knowingly allow their territory to be used for internationally wrongful acts using ICT" (UN General Assembly 2015). While the development of such international norms is currently being pursued, its effectiveness remains questionable. In the meantime, states are moving forward with their own strategies to combat and defend against cyber incidents.

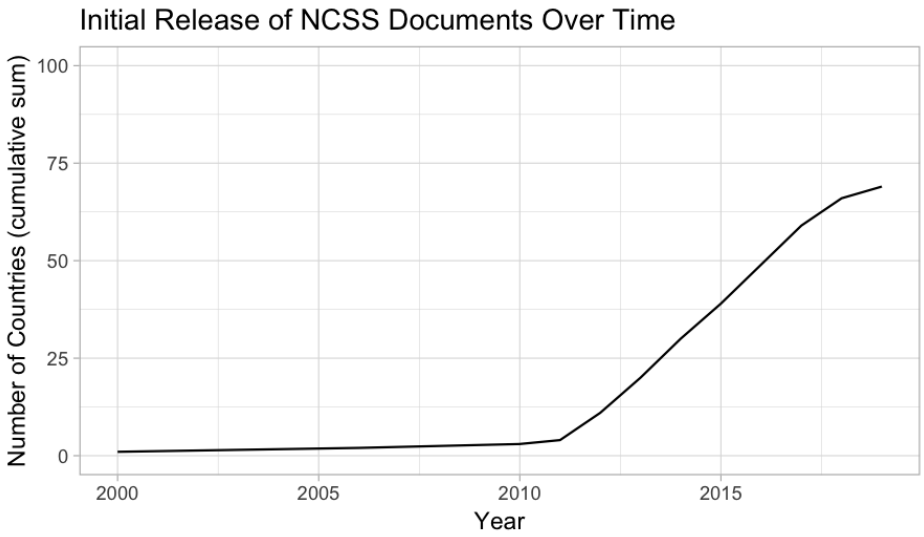

Figure 2: Timeline of countries' initial NCSS document releases as cumulative sums

Figure 2 shows the cumulative trend of initial release dates for states' national cybersecurity strategies. From 2012 and on, states rapidly began releasing their strategies addressing emerging threats in cyberspace. By 2012, enough "major" cyber incidents had occurred, likely motivating these strategy developments. However, despite growing threats within cyberspace, a majority of states still do not have a public strategy document regarding cybersecurity.

What role do these strategy documents have in practical terms and why are they made public? Independent from cybersecurity specifically, national security strategy documents are fairly common among states to develop and release to the public. Stolberg (2012) identifies three reasons for this. First, crafting such a document helps ground and focus the nation's strategy, making clear to various government departments and ministries the intent behind the elected government's strategic wishes (Stolberg 2012, 2). Second, a security strategy document assists the legislative body in better understanding the requested resources that require fiscal authorization, aiding in a smooth implementation of the strategic vision (Stolberg 2012, 3). Finally, such a document operates as strategic communication to both domestic constituents (i.e. voters, unions, lobbying groups) as

well as external audiences, such as foreign adversaries or states that pose a potential threat (Stolberg 2012, 3). Making a strategy document public offers a number of benefits, making it a useful tool in both domestic and foreign politics.

While these three reasons apply to broader national security strategy documents, the very same justifications apply to cybersecurity strategy documents as well. As a new and modern sub-domain within national security strategy, it makes sense to allot special attention to the issue of cybersecurity. In 2014, NATO established cyber defense as "part of NATO's core task of collective defence," clearly signalling to its members the significance of cybersecurity (Wales Summit Declaration 2014). Outlining national priorities when it comes to the cyber domain shapes both a nation's cyber defense policy as well as its cyber deterrence strategy. Not all strategic information is made public in these documents, of course; however, they operate as a means in communicating the state's offensive and defensive cyber capabilities against cyber incidents – critical information for effective deterrence.

The content of different states' strategies may vary in both detail and depth, but the mere existence of these documents is evidence of the growing demand for states to think more strategically about the increasing threats and vulnerabilities in cyberspace. To aid nations in this endeavor, international organizations such as the the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) have helped produce guides for developing robust national cybersecurity strategies.

Guide to Developing a National Cybersecurity Strategy (NCSS)

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is an international military organization located in Tallinn, Estonia whose mission is to "enhance capability, cooperation and information sharing between NATO, NATO member states and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation" (CCDCOE 2013, 2). It was established upon the initiative of Estonia (together with other nations) in 2008, one year after the Russian DDoS attacks targeting Estonia's infrastructure ("About Us", n.d.). It conducts the annual International Conference on Cyber Conflict (CyCon) and organizes international cyber defense exercises and simulations ("About Us", n.d.). The CCDCOE is responsible for producing the the Tallinn Manual 2.0, "the most comprehensive analysis on how existing international law applies to cyberspace" ("About Us", n.d.). As an organization separate from the NATO Command Structure, it is entirely staffed and funded by its members, including 22 sponsoring nations and three contributing participants.

In an effort to aid nations in their cyber security strategy development, the CCDCOE released a publication in 2013 titled, "National Cyber Security Guidelines" (CCDCOE 2013). Its aim is to "assist national policy planners in drafting, improving, implementing and evaluating their national cyber security strategies (NCSS) and other related documents, thereby achieving a higher level of protection against rapidly evolving cyber threats" (CCDCOE 2013, 6). Having such a document enables governments to identify strategic objectives, implement policies based on these objectives, and determine the resources needed to carry out such policies (CCDCOE 2013, 6). Similar to Stolberg (2012), this 2013 document highlights the role NCSSs have in communicating a cohesive strategy. Against the backdrop of increasing cyber incidents and NCSSs, states are demonstrating the importance of developing smart, comprehensive cybersecurity strategies.

The "National Cyber Security Guidelines" suggests that NCSSs consider the following aspects regarding cybersecurity: legal and regulatory measures, organizational measures, awareness raising measures and education, technological tools and measures, and critical infrastructure protection (CCDCOE 2013). While legal obligations, organizational structures, and technological capabilities are intuitively important for developing a national security strategy, awareness raising of and education for the public is rather unique to the realm of cybersecurity.[2] The guide suggests that nations consider the "necessity of bringing the relevant information, understanding and competence of cyber security to all levels of society" in order to "achieve a satisfactory level of cyber security awareness and competence in the society as a whole" (CCDCOE 2013, 17).

In 2018, the CCDCOE collaborated with other organizations including the International Telecommunication Union (ITU), the World Bank, Commonwealth Secretariat (ComSec), and the Commonwealth Telecommunications Organisation (CTO) to produce a more detailed "Guide To Developing a National Cybersecurity Strategy" (ITU et al. 2018). Its objective is to "to support national leaders and policy-makers in the development of defensive responses to cyber-threats, in the form of a National Cybersecurity Strategy, and in thinking strategically about cybersecurity, cyber-preparedness, response and resilience, building confidence and security in the use of information and communications technologies" (ITU et al. 2018, 5). It offers very detailed and comprehensive information on the subject of cybersecurity as well as the process of and "best practices" for developing a NCSS.

2. As an example, the general national security strategy documents of both the US and the UK do not mention public awareness campaigns or education and training for citizens in non-cyber security areas.

The "best practices" section includes several areas of focus, again touching on legal, organizational, and technological strategies. In addition to these, similar to the 2013 guide, there is also an area that addresses awareness and education, titled "capability and capacity building and awareness raising." This focus area includes the following best practices: develop a cybersecurity curricula, stimulate skills development and workforce training, and implement a coordinated cybersecurity awareness-raising programme. Further information on these can be seen in table 2.

Develop cybersecurity curriculua	"The Strategy should facilitate the development of school curricula with the aim of accelerating cybersecurity skills development and awareness throughout the formal education system. This should include developing dedicated cybersecurity curricula across primary and secondary schools, integrating cybersecurity courses in all computer science and IT programmes in higher education, and creating dedicated cybersecurity degrees and government apprenticeships...Additionally, the school curricula should foster awareness of and stimulate interest in cybersecurity career opportunities."
Stimulate skills development and workforce training	"The Strategy should address the development of cybersecurity training and skills development schemes for experts and non-experts in both public and private sectors...The Strategy should also foster initiatives, which aim to develop dedicated cybersecurity career paths, in particular for the public sector, and incentives to increase the supply of qualified cybersecurity professionals."
Implement a coordinated cybersecurity awareness-raising programme	"The Strategy should assign responsibility to coordinate cybersecurity awareness campaigns and activities at the national level to a competent authority...to develop and implement cybersecurity awareness programmes focusing on disseminating information about cybersecurity risks and threats, as well as about best practices for countering them. A cybersecurity awareness-raising programme could include awareness-raising campaigns aimed at the general public, children, digitally challenged, consumer focused education programmes, and awareness-raising initiatives among others, targeted at executives across public and private sectors."

Table 2: Best practices for capability and capacity building and awareness raising (ITU et al. 2018)

The document justifies the inclusion of these practices by noting the often overlooked "fundamental human element" at the core of cybersecurity (ITU et al. 2018, 45). This human element will be discussed further in the next section.

To conclude, the development of increasing cyber threats has led to the increasing development of national cybersecurity strategies. The need to formally address malicious cyber behavior is a strictly modern phenomenon, only manifesting in the last fifteen years or so. Whether states are facing cyber incidents from adversarial states or thrill-seeking hacktivists, the need for effective cyber defense and deterrence has become a high priority. Through these NCSS documents, we can observe how states aim to accomplish this task.

TOWARDS A USER-TAILORED APPROACH

The Reality of Human Error

The inclusion of the "human element" in NCSS document guidelines is both justified and critically important. Human error is responsible for a large proportion of successful cyber incidents, meaning that a reduction in human errors could significantly reduce the threat of malicious cyber operations. According to a 2014 IBM research report analyzing cyber incident data, "over 95 percent of all incidents investigated recognize 'human error' as a contributing factor" (IBM Global Technology Services 2014). These include system misconfiguration, poor patch management, use of default user names and passwords or easy-to-guess passwords, lost laptops or mobile devices, and disclosure of regulated information via use of an incorrect email address. However, "the most prevalent contributing human error? 'Double clicking' on an infected attachment or unsafe URL" (IBM Global Technology Services 2014).

Again, in 2014, an examination by Kadivar (2014) of 10 high-profile cyber "attacks" revealed that seven of the 10 incidents started with phishing or spear phishing (24). Phishing and spear phishing are methods that rely entirely on human vulnerabilities to gain sensitive data or gain unauthorized access to networks. In this scenario, an employee or user receives an email from a known entity or an entity that appears legitimate (i.e. supervisor, service provider, bank, etc.); the user either clicks on a URL that prompts them to enter sensitive data or an attachment (e.g. "security patch") that inserts malware into the system (Bhadane and Mane 2018). While phishing is a more general attack, spear phishing is a targeted attack against a particular individual using social engineering (i.e. psychological manipulation of a user).

Recent incidents provide further evidence of the role of human vulnerabilities in successful cyber operations. In 2015, Ukraine suffered a major attack on their power grid. Malware infected the systems of three Ukrainian power grid companies which wrecked their systems and caused a blackout for at least 224,000 people (Osawa 2017, 199; Lee, Assante, and Conway 2016). An investigation into the incident found that the "adversary delivered a targeted email with a malicious attachment that appeared to come from a trusted source to specific individuals within the organizations," thus allowing the attackers to gain system access (Lee, Assante, and Conway 2016, 11).

An intrusion of the German Bundestag's network in May 2015 also came about through the use of phishing methods. The attackers, believed to be Russia's APT28 or "Fancy Bear," gained access to the Bundestag's internal server and stole information ("Data Stolen" 2015). An article in *Die Zeit* describes how the attack began via email:

> On April 30, just over a week before Claudia Haydt tried to write to her acquaintance René, several German parliamentarians received an email at the same time. The sender's address ended with @un.org, making it look like it was from the United Nations. In truth, though, it was from the hackers, from a server that the Bundestag firewall did not recognize as problematic. The email subject line read, "Ukraine conflict with Russia leaves economy in ruins," and contained a link to a supposed UN bulletin. Those who clicked on the link ended up on an internet site that looked like a UN page, but actually surreptitiously installed malware onto the computer of the mail's recipient – a so-called trojan. (Beuth et al. 2017)

These same attackers are responsible for operations against other state governments. The White House and State Department under U.S. President Obama suffered a security breach of its unclassified system, revealing sensitive information (Brewster 2015). Again, methods included "spear phishing, where malicious yet legitimate-looking emails were sent to targets, ostensibly from State Department employees. When the files were opened, malware was launched at the victim's PC. The hackers managed to acquire persistence on the State Department network" (Brewster 2015). A European and North American foreign ministry were also targeted in 2018 in which the attackers again leveraged a phishing email (Lee, Harbison, and Falcone 2018). These are just a few cases of *many* where a state government is the target of a malicious phishing operation.

In addition to state governments, these operations are similarly conducted against political election campaigns, including, famously, the Democratic National Committee and John Podesta during the 2016 U.S. election as well as Emmanuel Macron in the 2017 French election. Thousands of emails and documents were stolen and released to the

public as a result of spearphishing techniques attributed to Russian cyberespionage groups (Nakashima 2016; Hern 2017). In the case of John Podesta, campaign chairman for Hillary Clinton in 2016, he received an "alarming email that appeared to come from Google" (Franceschi-Bicchierai 2016). After clicking the malicious link, Podesta unknowingly granted the attackers access to his account.

Businesses, banks, defense contractors, think tanks, and universities are also often the target of phishing and spearphishing operations (Department of Justice 2018; Kaspersky Lab 2019). In just 2019 alone, IBM's X-Force Threat Intelligence Index found that 29% of all security incidents globally involved compromises via phishing emails. Beyond phishing, the report also noted a 20% increase from 2017 in other human errors, such as "misconfigured cloud servers that include publicly accessible cloud storage, unsecured cloud databases, and improperly secured rsync backups, or open internet connected network area storage devices" (IBM Security 2019). These type of human errors contributed to 43% of the exposed records tracked in 2019.

The "human factor" plays a substantial role in the security and defense of critical information, systems, and infrastructure. Even high-profile users handling extremely sensitive government data are still susceptible to falling victim to social engineering and phishing techniques, let alone the millions of average employees working for various companies and organizations in less targeted sectors. Given the reality that human vulnerabilities, both psychological and technological, are heavily exploited in cyberspace by actors with malicious intent, how should states address these issues in their national cybersecurity strategy documents? According to the 2018 NCSS development guide, countries should develop cybersecurity curricula in schools, stimulate skills development and workforce training in cybersecurity, and implement coordinated cybersecurity awareness-raising programs (ITU et al. 2018).

Reducing Vulnerabilities via User Education and Training

In line with the general view that cyber deterrence requires a comprehensive and nuanced strategy (Wilner 2017; Lindsay 2015; Buchanan 2014; Tor 2017; Harknett, Callaghan, and Kauffman 2010), I argue that both deterrence and general defense in cyberspace would be greatly aided by a user-tailored approach that addresses these human vulnerabilities head-on. If human users are less susceptible to phishing attacks and social engineering, these methods no longer become useful strategies by malicious actors, thus debilitating their effectiveness. From a deterrence by denial standpoint, by denying the gains potential attackers would receive from such methods (e.g. denied entry to networks), they are deterred from initiating such operations in the first place.

In the summary of cyber deterrence provided by Ryan (2018), deterrence by denial is illustrated using the metaphor of a castle. Implementing defensive measures such as higher walls and stronger castle fortifications leads to deterrence if adversaries calculate that it is not worth the cost to attack. However, Ryan points out that in cyberspace, the goal is not necessarily to keep attackers out using a strong perimeter defense (as it is very difficult to do so) but rather to detect and "ban" them once they are inside before they can steal anything (2018, 334).

To expand on the castle metaphor further, I contend that the current situation is the following: An ordinary worker within the castle finds themself at the castle perimeter on some task for their job. An adversary, disguised as a familiar friend or ally, approaches the castle and tricks the castle worker into allowing the disguised adversary discreet entry into the castle. The disguised adversary is now inside the castle, obtaining and leaking invaluable amounts of sensitive information to the adversary's base, only being detected once it's too late. Rather than invest in training all castle workers to be suspicious and vigil about such malicious imposters, the castle lord instead invests in even stronger castle fortifications. In this situation, someone ought to tell the lord that, no matter how tall the walls are or wide the moat is, with clever tricks and social engineering, the weakest security link is, regrettably, the castle workers.

Of course, according to Ryan (2018), this castle metaphor could also include defensive measures *inside* the castle to catch such imposters. This is, and should continue to be, pursued as part of cyber deterrence. However, any cyber defense and deterrence strategy that ignores the training of its castle workers is a strategy just waiting to be exploited.

Rather than isolated castles, users today are working and operating in a very complex, interconnected world. Likewise, adversaries face complex and interconnected targets with numerous points of entry. As governments, businesses, and organizations worldwide increasingly digitize their workflow, data, and processes, targets of malicious cyber activity increase as well, especially from network intrusions (Maness, Valeriano, and Jensen 2019; Council of Foreign Relations, n.d.). To defend (and deter) adversaries disguised as friendly allies via phishing or spearphishing techniques, user training and education is essential. Further, to address improperly secured networks, a competent and reliable IT workforce is necessary to prevent discreet (or even overt) access to systems and networks. These strategies (education and training) are recommended by the 2018 Guide to Developing a National Cybersecurity Strategy. But important questions to investigate are, first, what do these strategies look like in practice and, second, how effective are they?

With regard to user training and education of public and private employees, many organizations already offer security awareness training (Caputo et al. 2014). According to

a Deloitte study (Subramanian and Robinson 2018), "Awareness training for state employees and contractors, at least annually, is now the established model in the vast majority of [US] states — 94 percent in 2018 compared to 84 percent in 2016" (25-26). While annual training may be common, researchers note a major drawback with this approach: retention. These once-a-year training sessions are likely ineffective without consistent recall and practice (Caputo et al. 2014). Many studies that investigate anti-phishing user training methods concur that continuous learning with repeated exposure and interventions is much more effective in reducing phishing susceptibility (Kumaraguru et al. 2009; Alnajim and Munro 2009; Lastdrager et al. 2017).

"Embedded training" is such an approach that offers continuous learning about phishing threats. The idea is that employees routinely receive simulated phishing emails; if they click the link or provide sensitive information according to the simulated phishing email, they will receive a message that explains to them the potential consequences of what they just did and how to better discern phishing emails from legitimate ones. This is a real-time training method that teaches users about phishing threats the moment it happens – a method shown in experimental studies to improve phishing detection (Kumaraguru et al. 2009; Alnajim and Munro 2009).

A study conducted on employees of a US hospital found that, while the embedded training (i.e. consistent simulated phishing email campaigns) appeared to reduce phishing clicks over time, a one-off mandatory training for particularly susceptible users did not affect their behavior (Gordon et al. 2019). This lends further support to the positive effect of continuous learning over infrequent, isolated training attempts.

Another study by Lastdrager (2017) examined the effects of educating *children* in their schools on their susceptibility to phishing attempts. Results reveal that training children improved their abilities to detect phishing emails in the short-term; however, knowledge retention proved difficult and scores dropped after four weeks (Lastdrager et al. 2017). Lastdrager (2017) concludes that continuous training is indeed a solution for effective anti-phishing training, but recognizes the monetary costs of such an approach.

With regard to a robust cybersecurity industry workforce, some countries have already taken steps to incentivize careers in cybersecurity. For examples, the US Department of Homeland Security created the Cybersecurity Education and Awareness Branch which is "committed to strengthening the nation's cybersecurity workforce" and offers a National Professionalization and Workforce Development Program aimed to "facilitate a robust and ready cybersecurity workforce" (Department of Homeland Security 2019). Such national attempts help address cyber competency gaps, resulting in a stronger defense against

other human-related errors such as system misconfiguration and poor patch management.

How might user training and a robust cybersecurity workforce lead to an effective deterrence of malicious cyber operations? It is first important to note that this approach is more specifically tailored to network intrusions and infiltrations – arguably the more threatening and damaging type of cyber incidents. By reducing the volume of successful intrusions and infiltrations through a high collective phishing immunity, the benefits gained through such strategies by attackers drop significantly, thus deterring potential aggressors from pursuing phishing and spearphishing tactics in the first place. In the case of a successful intrusion, however, deterrence by punishment still faces many challenges. Deterrence by initially denying access through a competent and vigilant human firewall avoids these challenges altogether.

MAPPING NATIONAL CYBERSECURITY STRATEGIES

How do states address the role of users (i.e. citizens) in their national cybersecurity strategies in practice? I argue that user-tailored education and workforce training are critically important for cyber deterrence and defense. Unlike other security domains, the cybersecurity realm involves billions of ordinary – and vulnerable – citizens, some of whom may be important gatekeepers to sensitive information. By decreasing users' susceptibility to socially and psychologically exploitative tactics through education, employee training, and public awareness, threats to critical information and infrastructure can be significantly reduced. Further, a robust cybersecurity workforce likewise reduces other human errors that leave networks vulnerable to intrusions and infiltrations. The question now is, are states addressing these vulnerabilities in their own national cybersecurity defense strategies?

Design and Method

In order to assess whether states are considering the role of human errors in their strategies, I utilized the CCDCOE library to examine all recent and available NCSS documents.[3] The CCDCOE library includes a specific document category, "cyber security strategies," for each country. Most countries offer official English-language versions of the text; however,

3. For document links that were broken, I found the correct document on the website of The European Union Agency for Cybersecurity (ENISA).

several do not. Due to a number of limitations, out of the 69 available documents, I only analyzed the 51 English documents, plus the documents of Russia and Germany.[4] Therefore, the total number of observations in this analysis is 53, leaving 16 more documents that could be translated and added to the analysis in the future.

I examined these texts using a coding scheme I developed based on the "best practices" discussed earlier in the paper (see table 2). This coding scheme can be found in the appendix. To summarize, there are three categories that capture the user-tailored approach: education, workforce, and awareness. In each category, there are topics worth points if mentioned in the document. Education has a total of five points, workforce has a total of three points, and awareness has a total of three points.[5] Further, measures for breadth and depth are calculated based on these points in order to capture the level of detail provided by the document. These points are recorded in a database (available upon request). Additionally, to create figure 2 from earlier in the paper, I included the year a country *first* released a public document, which may differ from the year of their most recent strategy document.

I use these three categories – education, workforce, and awareness – to address the different components of the strategic argument I am making. 'Education' includes curricula changes to primary and secondary schools in addition to changes made broadly across higher education programs. It also includes the education of both public and private sector employees via training efforts. These initiatives capture the formal education and training of non-specialized citizens at large.

The 'workforce' category includes taking steps to create a pathway for a competent cybersecurity workforce. This includes formal degrees, apprenticeship, and/or certification opportunities for young people starting their careers (or those retraining) as well as additional training for specialists already working in the cybersecurity field. There may also be other incentives included for pursuing a career in cybersecurity or simply an expressed desire to develop such a workforce.

Finally, the 'awareness' category includes public awareness campaigns (e.g. marketing and public service campaigns, website portals) that offer less formal access to critical information regarding cybersecurity. Additional programming outside of a campaign may also offer similar services to citizens (i.e. other events or courses offered by the state). It

4. I used Google Translate to help identify keywords and relevant context according to the coding scheme used.

5. To test whether the variation in points among these categories affects the overall analysis, I also code the 'education' category using three points.

may also be the case that a specific authority has been charged with carrying out these efforts.

Altogether, analyzing NCSS documents based on these elements offers a compelling way to assess whether or not countries are addressing the role of humans and users in their overall cyber strategy. While others may prefer to categorize these elements differently, the overall "score" should be rather resilient to cosmetic changes in the coding scheme.

Results

After coding 53 countries' NCSS documents, there is wide variation between countries and the extent in which they address these three components of a user-tailored approach to cybersecurity. Figure 3 illustrates the rather bimodal distribution of countries' overall sum of points (hereafter referred to as their "score"). Based on the 5-point scoring system for the "education" category, the mean score is 6.17 with a median of 7 and mode of 7. However, when coding the documents based on a 3-point system for the education category, the bimodal trend remains. For this analysis, I continue to use the 5-point system as it offers more nuance without contradicting the 3-point trend. The 5-point system simply emphasizes a trend that already exists while offering more context and detail.

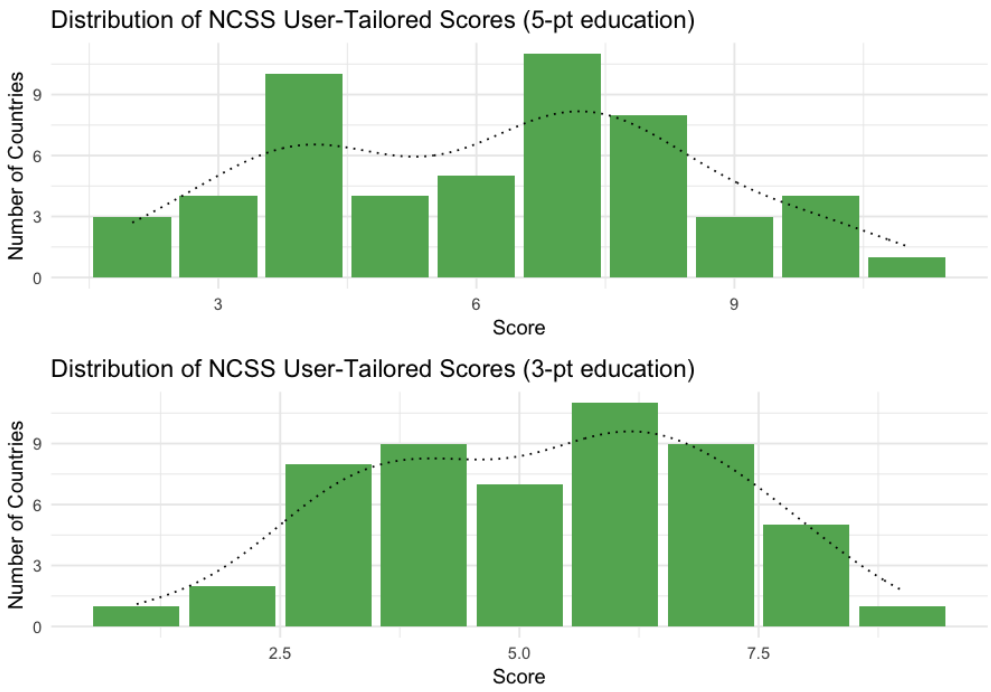

Figure 3: Overall score distribution, 5-point vs. 3-point "education" category

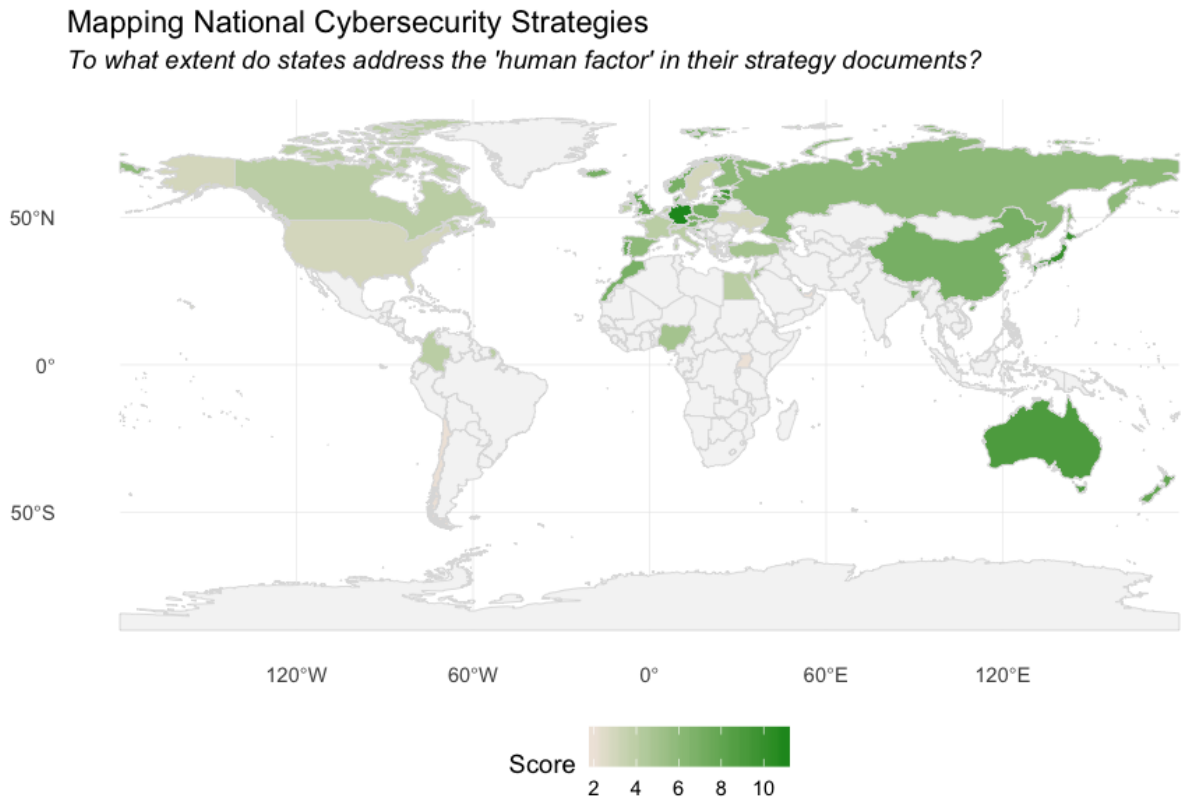

Figure 4: World map of countries' overall score of their user-tailored approaches

Table 3 in the appendix lists the overall scores for each country which forms the basis for the map in figure 4. While these scores offer a convenient "quick-look" at which countries more strongly incorporate a user-tailored approach in their NCSS, they do not reveal their coverage or depth. In order to better examine the level of detail of these documents, figure 5 represents the calculated "breadth" and "depth" variables. Seventy-five percent of observed countries address all of the three categories, at least minimally (i.e. receiving 1 point). However, only one country – Germany – receives full points in all three categories; 49% reach full points in at least one category while the remaining 49% do not receive full points in any category.

Overall, the breadth and depth of these total scores offer interesting insights. The high breadth suggests that countries are generally aware of these human factors related to cybersecurity and attempt to address them from different angles; however, the lower depth implies that there is room for improvement in the extent to which states could approach the strategy.

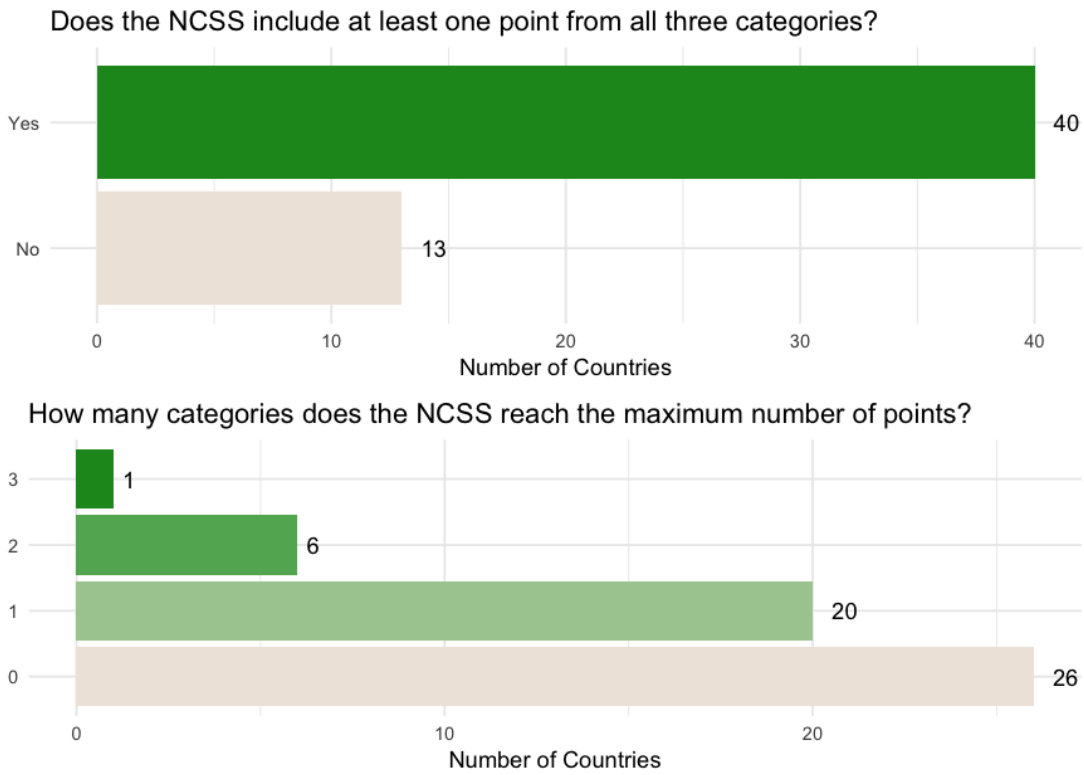

Figure 5: Breadth and depth distributions

Breakdown by User-Tailored Subcategories

The distribution of points in each of the three categories is further illuminating. As is seen in the top portion of figure 6, 41.5% of states receive full points in the workforce category. This being the category where most states maximize their points, we can gather that many states do address the size and competence of their cybersecurity workforce, particularly through training those already in the field (according to the breakdown of subcategories in the lower portion of figure 6).

Apart from where states maximize their approach according to these user-tailored categories, it is especially clear from figure 6 that states overwhelmingly include public awareness campaigns in their strategies. While they may not always specify a particular authority in charge or highlight additional awareness initiatives, at the bare minimum, all but five states under observation mention public awareness of cyber threats in their strategy documents.

The "Private/Public Sector Training" subcategory offers further insights. While an overwhelming majority of states mention the training of at least one sector (1 point) of non-experts in cybersecurity, only 22 countries make a point to include the training of

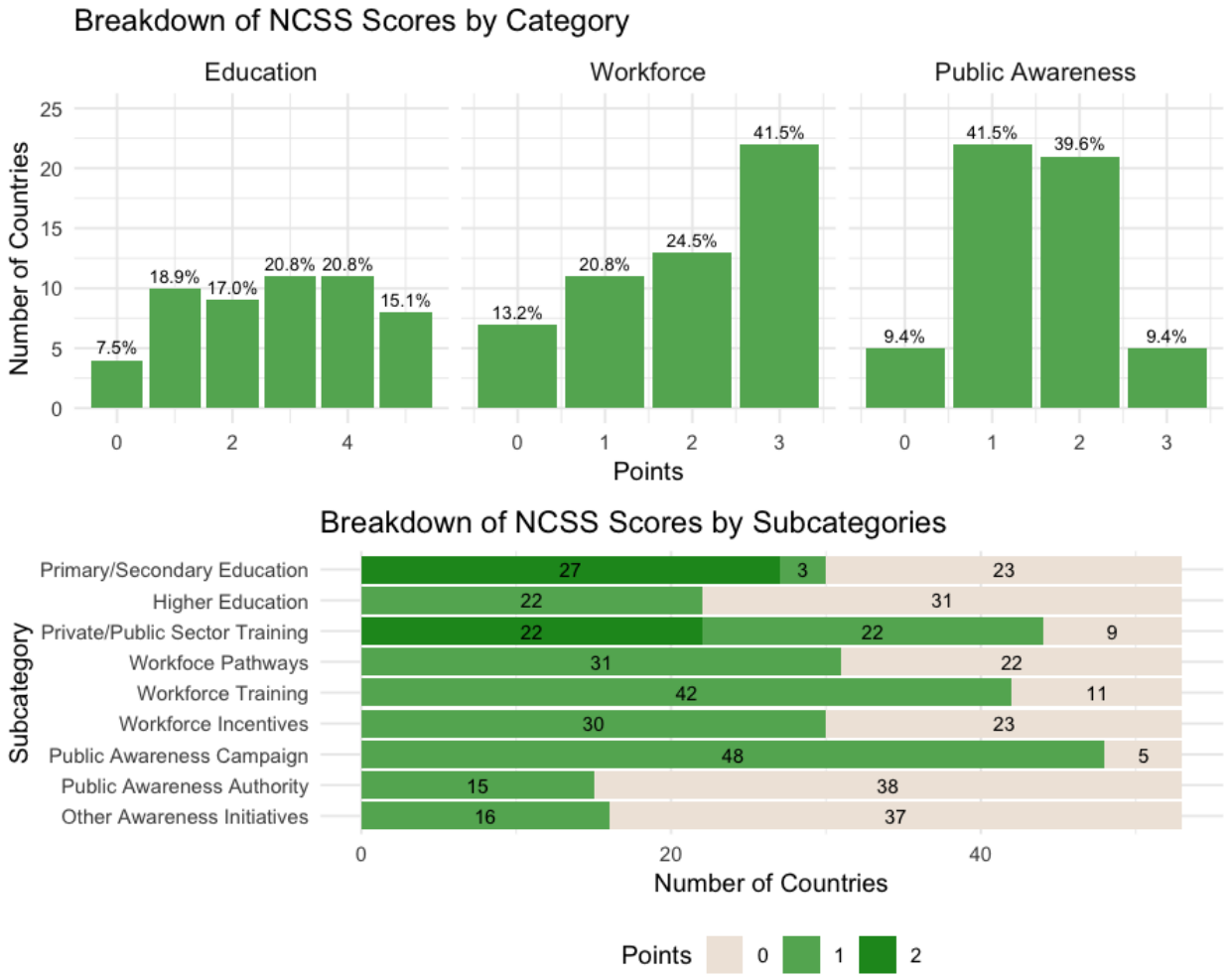

Figure 6: Score breakdown by categories and subcategories

non-experts from both sectors. Training law enforcement, government officials, and other public employees is rather common; however, the inclusion of private sector employees occurs less frequently. While state secrets and important government information are largely protected by public officials, employees working with critical infrastructure or in defense or financial industries are often private yet also important to a nation's cyberdefense.

This breakdown additionally identifies areas where states could improve in each category. However, it will become increasingly important to conduct and consult impact studies so that states can maximize their strategy in areas that are proven to be most effective (e.g. effective training methods, effecting marketing campaigns, etc.).

To see which countries are most similar to each other, table 3 presents a column listing the country (or countries) with the most similar scoring based on their subcategory points. This similarity was determined by calculating the Euclidean distance between each country and extracting the country-pair with the smallest distance. From this calculation, we can gather that Germany's NCSS document approaches the human factor more similarly to that of Japan and Trinidad Tobago than it does to, say, France. We can glean from this that regional proximity does not necessarily indicate closeness in terms of strategy.

A Closer Look at the European Union

Europe is the most represented region among the NCSS documents under observation. Seventy-five percent of European countries have public NCSS documents (among these, 23 out of 28 EU countries in particular). Meanwhile, only 15%, 29%, 31%, and 23% of countries are represented in Africa, the Americas, Asia, and Oceania, respectively.

In looking specifically at how the EU compares to the rest of the world, the mean score of EU countries is 6.65 while the mean of non-EU countries is 5.8 (a difference of 0.85). EU countries have only slightly better scores on average than non-EU countries. A t-test between these two samples (EU and non-EU) indicates no significant statistical difference between the average scores. However, it is important to remember that this comparison is being made only among 53 countries.

The EU has offered a cybersecurity strategy of its own. Using the same coding procedure for this document, the EU's overall score is 7. While EU countries exhibit a wide variation of scores (from 3 to 11), the median and mode of EU countries is 7 and the mean is 6.7 – on average, very similar to the single EU strategy document. While regional proximity does not necessarily indicate strategic similarities, perhaps international in-

stitutions – such as that of the EU – have some impact on strategy convergence among members.

CONCLUSION

The cyber domain has become an increasingly utilized space for conflict among states. Unlike physical battlefields where combatants are generally limited to militaries and actors on the ground, cyberspace is made up of billions of unknowing participants whose human vulnerabilities could be exploited by malicious actors. Every person with a device connected to a network, especially those working at or with high-value targets, is on the front line of this developing conflict space.

Ordinary citizens on cyber "front lines" is not mere hyperbole; most high-profile cyber incidents were successful due to phishing tactics that used social engineering to take advantage of user vulnerabilities and gain unauthorized network access. One wrong click by the right person could cause irreversible damage to a nation's security. Civilians are not required to learn military strategy or enemy tactics in conventional warfare; however, in today's interconnected cyber world, it is in the interest of states' national security to ensure their citizens are trained in and made aware of basic cybersecurity issues in order to both strengthen cyber defense as well as cyber deterrence.

Scholars have debated the feasibility of cyber deterrence and whether or not it can be effectively implemented. This paper argued a user-tailored approach that aims to strengthen the "human firewall" would greatly aid a deterrence by denial strategy. If malicious actors are denied network access due to users' reduced vulnerability via education and training, the benefits gained no longer outweigh the costs, resulting in deterred cyber operations (at least of those operations that exploit such human weaknesses).

With this perspective in mind, I analyzed 53 national cybersecurity strategies (NCSS) to assess weather states are indeed taking a user-centered approach towards cybersecurity and to what extent. Overall, most countries recognize the human component in their strategies and mention tactics related to education, workforce training, and public awareness, at least minimally. However, fewer countries address all three areas with much depth, leaving great room for improvement in their strategic approaches.

Of course, the strategies analyzed here are simply those publicly written on paper; whether or not countries are actually implementing these approaches is another question entirely. However, the first step towards formulating an effective strategy towards this new conflict domain involves a strategic vision which is what this paper assesses. Most countries have still not released a public NCSS document, so this analysis was lim-

ited to only those documents that were available and, further, those that were available in English.

Future research could improve on and continue this analysis in a number of ways. First, the remaining 16 documents from non-native-English speaking countries could be translated (or read by a native speaker) in order to code those strategies and include them here. The coding scheme could also be improved with more detail and direction to avoid unreliability between different coders and among individual coders. Beyond the present analysis, future research could look further at the impact of user-tailored strategies. First, how well do states put these on-paper approaches into action and, second, are they effective? Does user training and education reduce network intrusions via phishing? Does a larger, more competent cybersecurity workforce reduce malicious cyber incidents? Does a cyber-aware public increase resilience against cyber operations? Answering these questions will help determine whether or not cyber deterrence by denial actually works using these user-tailored methods.

This analysis is a first step in mapping out the current landscape of national cybersecurity strategies. As state behavior and capabilities in cyberspace continue to emerge and develop, it will become increasingly important to monitor defense and deterrence strategies in response to growing threats and challenges. While user-centered approaches may face practical costs and obstacles, they may nevertheless prove to be a worthy deterrence investment in the face of severe security consequences otherwise.

REFERENCES

"About Us". n.d. *The NATO Cooperative Cyber Defence Centre of Excellence*. Accessed 3 December. https://ccdcoe.org/about-us/.

Alnajim, Abdullah, and Malcolm Munro. 2009. "An anti-phishing approach that uses training intervention for phishing websites detection." In *6th International Conference on Information Technology: New Generations,* 405–410. IEEE.

Beuth, Patrick, Kai Biermann, Martin Klingst, and Holger Stark. 2017. "Cyberattack on the Bundestag: Merkel and the Fancy Bear". *Die Zeit*. 12 May. http://www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia/komplettansicht.

Bhadane, Aniket, and Sunil B. Mane. 2018. "State of Research on Phishing and Recent Trends of Attacks." *i-manager's Journal on Computer Science* 5 (4): 14–35. doi:10.26634/jcom.5.4.14608.

Brewster, Thomas. 2015. "Russians Hacked White House Via State Department, Claims Report". *Forbes*. 8 April. https://www.forbes.com/sites/thomasbrewster/2015/04/08/russians-hacked-white-house-cnn/%7B%5C#%7D29bcd08b60cb.

Buchanan, Ben. 2014. "Cyber Deterrence Isn't MAD; It's Mosaic." *Georgetown Journal of International Affairs,* no. 2014: 130–140.

Caputo, Deanna D., Shari Lawrence Pfleeger, Jesse D. Freeman, and M. Eric Johnson. 2014. "Going Spear Phishing: Exploring Embedded Training and Awareness." *IEEE Security and Privacy* 12 (1): 28–38. doi:10.1109/MSP.2013.106.

CCDCOE. 2013. "National Cyber Security Strategy Guidelines." https://www.gov.uk/government/uploads/system/uploads/attachment%7B%5C_%7Ddata/file/567242/national%7B%5C_%7Dcyber%7B%5C_%7Dsecurity%7B%5C_%7Dstrategy%7B%5C_%7D2016.pdf.

Council of Foreign Relations. n.d. "Cyber Operations Tracker." *Council of Foreign Relations.* https://www.cfr.org/interactive/cyber-operations/turla.

Crosston, Matthew D. 2011. "World Gone Cyber MAD: How "Mutually Assured Debilitation" is the Best Hope for Cyber Deterrence." *Strategic Studies Quarterly* 5 (1): 100–116.

"Data Stolen During Hack Attack on German Parliament, Berlin Says". 2015. *Deutsche Welle*. 29 May. May. https://p.dw.com/p/1FZHo.

Department of Homeland Security. 2019. “Cyber Education and Awareness". Accessed December 3. https://www.dhs.gov/cisa/cyber-education-and-awareness.

Department of Justice. 2018. “North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions". 6 September. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

Federal Ministry of the Interior. 2011. “Cyber Security Strategy for Germany". February. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber%7B%5C_%7DSecurity%7B%5C_%7DStrategy%7B%5C_%7Dfor%7B%5C_%7DGermany.pdf?%7B%5C_%7D%7B%5C_%7Dblob=publicationFile%7B%5C%%7D0Apapers3://publication/uuid/57A9D0C2-1F4A-438A-8FE3-37E19C2F8F44.

Franceschi-Bicchierai, Lorenzo. 2016. “How Hackers Broke Into John Podesta and Colin Powell’s Gmail Accounts". *Vice*. 20 October. https://www.vice.com/en%7B%5C_%7Dus/article/mg7xjb/how-hackers-broke-into-john-podesta-and-colin-powells-gmail-accounts.

Geers, Kenneth. 2010. “The Challenge of Cyber Attack Deterrence.” *Computer Law and Security Review* 26 (3): 298–303. doi:10.1016/j.clsr.2010.03.003. http://dx.doi.org/10.1016/j.clsr.2010.03.003.

Gordon, William J., Adam Wright, Robert J. Glynn, Jigar Kadakia, Christina Mazzone, Elizabeth Leinbach, and Adam Landman. 2019. “Evaluation of a Mandatory Phishing Training Program for High-Risk Employees at a US Healthcare System.” *Journal of the American Medical Informatics Association* 26 (6): 547–552. doi:10.1093/jamia/ocz005.

Harknett, Richard J, John P Callaghan, and Rudi Kauffman. 2010. “Journal of Homeland Security and Leaving Deterrence Behind : War-Fighting and National Cybersecurity Leaving Deterrence Behind : War-Fighting and National Cybersecurity.” *Journal Of Homeland Security And Emergency Management* 7 (1).

Hathaway, Oona A, Rebecca Crootof, William Perdue, Philip Levitz, Haley Nix, Aileen Nowlan, and Julia Spiegel. 2012. “The Law of Cyber-Attack.” *California Law Review* 100 (4): 1–60. doi:https://doi.org/10.15779/Z38CR6N.

Hern, Alex. 2017. “Macron Hackers Linked to Russian-affiliated Group Behind US Attack". *The Guardian*. 8 May. http://www.theguardian.com/world/2017/may/08/macron-hackers-linked-to-russian-affiliated-group-behind-us-attack.

Iasiello, Emilio. 2013. “Is Cyber Deterrence an Illusory Course of Action?” *Journal of Strategic Security* 7 (1): 54–67. doi:10.5038/1944-0472.7.1.5.

IBM Global Technology Services. 2014. “IBM Security Services 2014 Cyber Security Intelligence Index". doi:10.1016/j.inffus.2007.06.002.

IBM Security. 2019. “X-Force Threat Intelligence Index 2019". https://www.ibm.com/downloads/cas/ZGB3ERYD.

International Telecommunication Union. 2019. “Measuring Digital Development: Facts and Figures 2019.” https://www.itu.int/en/mediacentre/Documents/MediaRelations/ITU%20Facts%20and%20Figures%202019%20-%20Embargoed%205%20November%201200%20CET.pdf.

International Telecommunication Union (ITU), The World Bank, Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). 2018. “Guide To Developing a National Cybersecurity Strategy.”

Kadivar, Mehdi. 2014. “Cyber-Attack Attributes.” *Technology Innovation Management Review,* no. November: 22–28.

Kaspersky Lab. 2019. “Understanding Security of the Cloud: from Adoption Benefits to Threats and Concerns". https://www.kaspersky.com/blog/understanding-security-of-the-cloud/?utm%7B%5C_%7Dsource=pr-media%7B%5C&%7Dutm%7B%5C_%7Dmedium=partner%7B%5C&%7Dutm%7B%5C_%7Dcampaign=gl%7B%5C_%7Db2b-cloud-mini-report%7B%5C_%7Dkk0084%7B%5C_%7Dorganic%7B%5C&%7Dutm%7B%5C_%7Dcontent=link%7B%5C&%7Dutm%7B%5C_%7Dterm=gl%7B%5C_%7Dpr-media%7B%5C_%7Dorganic%7B%5C_%7Dkk0084%7B%5C_%7Dlink%7B%5C_%7Dpartner%7B%5C_%7Db2b-cloud-mini-report.

Kugler, Richard L. 2011. “Deterrence of cyber attacks.” *Cyberpower and National Security:* 309–340. doi:10.2307/j.ctt1djmhj1.18.

Kumaraguru, Ponnurangam, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. 2009. “School of Phish: A Real-World Evaluation of Anti-Phishing Training.” In *Symposium on Usable Privacy and Security (SOUPS).* Mountain View, CA USA. doi:10.1145/1572532.1572536.

Lastdrager, Elmer, Inés Carvajal Gallardo, Marianne Junger, and Santa Clara. 2017. “How Effective is Anti-Phishing Training for Children?” In *Proceedings of the thirteenth Symposium on Usable Privacy and Security, SOUPS 2017.* Berkely, CA: USENIX Association.

Lee, Bryan, Mike Harbison, and Robert Falcone. 2018. “Sofacy Attacks Multiple Government Entites". *Unit 42*. 28 February. https://unit42.paloaltonetworks.com/unit42-sofacy-attacks-multiple-government-entities/.

Lee, Robert M., Michael J. Assante, and Tim Conway. 2016. "Analysis of the Cyber Attack on the Ukrainian Power Grid". *SANS-ICS and E-ISAC*. 18 March. https://ics.sans.org/media/E-ISAC%7B%5C_%7DSANS%7B%5C_%7DUkraine%7B%5C_%7DDUC%7B%5C_%7D5.pdf.

Libicki, Martin C. 2018. "Expectations of Cyber Deterrence." *Strategic Studies Quarterly* 12 (4): 44–57.

Lindsay, Jon R. 2015. "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack." *Journal of Cybersecurity* 1 (1): 53–67. doi:10.1093/cybsec/tyv003.

Maness, Ryan C., Brandon Valeriano, and Benjamin Jensen. 2019. "The Dyadic Cyber Incident and Dispute Data (DCID), version 1.5". doi:10.1017/CBO9781107415324.004. arXiv: arXiv:1011.1669v3. https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset.

Nakashima, Ellen. 2016. "Russian Government Hackers Penetrated DNC, Stole Opposition Research on Trump". *The Washington Post*. 14 June. https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html.

Osawa, Jun. 2017. "The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?" *Asia-Pacific Review* 24 (2): 113–131. doi:10.1080/13439006.2017.1406703.

Owens, William A, Kenneth W Dam, and Herbert S Lin. 2009. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Edited by William A Owens, Kenneth W Dam, and Herbert S Lin. Washington, D.C.: The National Academic Press.

Ryan, N. J. 2018. "Five Kinds of Cyber Deterrence." *Philosophy and Technology* 31 (3): 331–338. doi:10.1007/s13347-016-0251-1.

Schulze, Matthias. 2019. "Cyber Deterrence is Overrated". https://www.swp-berlin.org/fileadmin/contents/products/comments/2019C34%7B%5C_%7Dshe.pdf.

Singer, Peter W., and Allan Friedman. 2013. "The World Wide What? Defining Cyberspace." In *Cybersecurity and Cyberwar: What Everyone Needs to Know*, 12–66.

Stolberg, Alan G. 2012. "How Nation-States Craft National Security Strategy Documents". doi:10.1093/oxfordhb/9780199219322.003.0032.

Subramanian, Srini, and Doug Robinson. 2018. "2018 Deloitte-NASCIO Cybersecurity Study".

Theohary, Catherine A. 2018. “Defense Primer: Cyberspace Operations". *Congressional Research Service*. 18 December. www.crs.gov%7B%5C%%7D7C7-5700.

Tor, Uri. 2017. “‘Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence.” *Journal of Strategic Studies* 40 (1-2): 92–117. doi:10.1080/01402390.2015.1115975. http://dx.doi.org/10.1080/01402390.2015.1115975.

UN General Assembly. 2015. “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” In *A/70/174*. http://www.un.org/ga/search/view%7B%5C_%7Ddoc.asp?symbol=A/70/174.

Wilner, Alex. 2017. “Cyber Deterrence and Critical-Infrastructure Protection: Expectation, Application, and Limitation.” *Comparative Strategy* 36 (4): 309–318. doi:10.1080/01495933.2017.1361202. https://doi.org/10.1080/01495933.2017.1361202.

APPENDIX

Coding NCSS Documents: Coding scheme created based on "best practices" from the 2018 Guide to Guide To Developing a National Cybersecurity Strategy (ITU et al. 2018).

Education = 5 points

- 2 points: Cybersecurity curricula across primary and secondary schools
  - "All levels of school" or stating specifically each individually; one of either = 1
  - Excludes simple "training"
- 1 point: Cybersecurity in higher education curricula
  - General curriculum, not specific cyber-career
- 2 points: Training for non-expert employees (private/public, including teachers)
  - 1 point for just a subset mentioned for training, e.g. only teachers, law enforcement

Search terms: curricul, educat, train, school

Workforce = 3 points

- 1 point: Cybersecurity degrees/courses/apprenticeships/general accreditation
- 1 point: Training for experts already in the field
- 1 point: Incentives for careers and professionals in cybersecurity
  - Includes even simply "develop a workforce" (e.g. Qatar)

Search terms: workforce, career, degree, appren, professional, specialists, training

Awareness = 3 points

- 1 point: Assigned authority responsible for public awareness campaigns
- 1 point: Public awareness campaigns in general
- 1 point: Other educational programs outside of education and training for the public

Search terms: aware, public, campaign

Level of Detail

- Breadth: Does it include at least one point from all three categories? (Yes/No = 1/0)
- Depth
  - 0: reaches no max pts in all categories
  - 1: reaches max pts in 1 category
  - 2: reaches max pts in 2 categories
  - 3: reaches max pts in 3 categories

	Country	Overall Score	Breadth	Depth	Most Similar Countries
1	Germany	11	1	3	Estonia, Japan, Luxembourg, Trinidad & Tobago
2	Estonia	10	1	2	Trinidad & Tobago
3	Japan	10	1	2	Estonia, Germany, Latvia, Luxembourg, Trinidad & Tobago
4	Luxembourg	10	1	2	Estonia, Germany, Japan, Latvia, Trinidad & Tobago
5	Trinidad & Tobago	10	1	2	Estonia
6	Australia	9	1	2	Singapore
7	Latvia	9	1	1	Malta
8	Samoa	9	1	1	Portugal
9	Croatia	8	1	1	Czechia
10	Jamaica	8	1	1	Malta
11	Malta	8	1	1	Latvia, Poland
12	Mauritius	8	1	0	Austria, Bangladesh, Iceland
13	New Zealand	8	1	1	Qatar, United Kingdom
14	Portugal	8	1	1	Czechia, Samoa
15	Qatar	8	1	1	New Zealand, United Kingdom
16	United Kingdom	8	1	1	New Zealand, Qatar
17	Austria	7	1	0	Mauritius
18	Bangladesh	7	1	0	Mauritius, Slovenia
19	China	7	1	1	New Zealand, Qatar, United Kingdom
20	Czechia	7	1	1	Croatia, Portugal
21	Denmark	7	1	0	Iceland, New Zealand, Qatar, United Kingdom
22	Iceland	7	1	0	Mauritius, Slovenia
23	Lithuania	7	0	1	Malta
24	Morocco	7	1	1	Nigeria, Norway
25	Norway	7	1	1	New Zealand, Qatar, United Kingdom
26	Poland	7	1	1	Malta, New Zealand, Qatar, United Kingdom
27	Singapore	7	1	2	Australia, Spain
28	Finland	6	0	1	China
29	Russia	6	1	0	Georgia, Italy, Switzerland
30	Slovakia	6	0	0	Iceland
31	Slovenia	6	1	0	Bangladesh, Iceland
32	Spain	6	1	1	Nigeria
33	Jordan	5	1	0	Egypt
34	Montenegro	5	0	0	Netherlands, Slovenia
35	Nigeria	5	1	1	Spain
36	Turkey	5	1	0	Italy, Switzerland
37	Canada	4	1	0	Netherlands
38	Colombia	4	1	0	Sweden
39	Egypt	4	1	0	Jordan
40	France	4	0	0	Ukraine
41	Georgia	4	1	0	Sweden
42	Ireland	4	0	0	Chile, Jordan, Uganda
43	Italy	4	1	0	Switzerland
44	Netherlands	4	1	0	Canada
45	South Korea	4	0	0	United Arab Emirates
46	Switzerland	4	1	0	Italy
47	Greece	3	0	1	Ukraine
48	Sweden	3	1	0	Colombia, Georgia, Italy, Switzerland
49	Ukraine	3	0	0	Chile, France
50	United States	3	0	1	Nigeria
51	Chile	2	0	0	Ukraine
52	Uganda	2	0	0	Chile, Ireland
53	United Arab Emirates	2	0	0	Chile, South Korea

Table 3: Scoring results of NCSS documents by country