Research Paper

Breaking botnets: A quantitative analysis of individual, technical, isolationist, and multilateral approaches to cybersecurity

Justin K. Haner 1,* and Robert K. Knake2,3

1Department of Political Science, Northeastern University, Boston, MA, USA; 2The Belfer Center for Science and International Affairs, Harvard University, Cambridge, MA, USA; and 3The Council on Foreign Relations, New York, NY, USA

*Correspondence address. Department of Political Science, Northeastern University, 960A Renaissance Park, 360 Huntington Avenue, Boston, MA 02115, USA. Tel: 617-373-2796; E-mail: haner.j@northeastern.edu

Received 25 March 2020; revised 27 October 2020; accepted 22 January 2021

Abstract
Malicious networks of botnets continue to grow in strength as millions of new users and devices connect to the internet each day, many becoming unsuspectingly complicit in cyber-attacks or unwitting accomplices to cybercrimes. Both states and nonstate actors use botnets to surreptitiously control the combined computing power of infected devices to engage in espionage, hacking, and to carry out distributed denial of service attacks to disable internet-connected targets from businesses and banks to power grids and electronic voting systems. Although cybersecurity professionals have established a variety of best practices to fight botnets, many important questions remain concerning why levels of botnet infections differ sharply from country to country, as relatively little empirical testing has been done to establish which policies and approaches to cybersecurity are actually the most effective. Using newly available time-series data on botnets, this article outlines and tests the conventionally held beliefs and cybersecurity strategies at every level—individual, technical, isolationist, and multilateral. This study finds that wealthier countries are more vulnerable than less wealthy countries; that technical solutions, including patching software, preventing spoofing, and securing servers, consistently outperform attempts to educate citizens about cybersecurity; and that countries which favor digital isolation and restrictions on internet freedom are not actually better protected than those who embrace digital freedom and multilateral approaches to cybersecurity. This latter finding is of particular importance as China’s attempts to fundamentally reshape the internet via the “Digital Silk Road” component of the Belt and Road Initiative will actually end up making both China and the world less secure. Due to the interconnected nature of threats in cyberspace, states should instead embrace multilateral, technical solutions to better govern this global common and increase cybersecurity around the world.

Key words: cybersecurity; botnets; bots; malware; multilateralism; DDoS; distributed denial of service; cyber; cyber policy; internet freedom; internet governance; global governance; cybercrime; cyberspace; routine activity theory; software piracy; BCP-38, anti-spoofing protocol

Introduction
Citizens of Estonia woke on 27 April 2007 to find themselves the target of the world’s first major cyber-attack against a sovereign state. Panic ensued as the banking, news, communications, and public sectors of Estonia were inundated by 400 times their normal internet traffic, overwhelming their systems. The traffic was...
seemingly flooding in from all over the world [1]. By the time they could fend off the attack, which is believed to have been orchestrated by Russia in retaliation for the removal of a Russian soldier’s statue from a prominent position in the capital Tallin, weeks had passed, and both public confidence in these institutions and tens of millions of dollars in revenue were lost [2]. Estonia had faced the world’s first major distributed denial of service (DDoS) attack. A DDoS attack uses a large amount of computing power drawn from thousands or even millions of devices to intentionally overload a targeted system and either deny or disrupt its service. DDoS attacks are typically carried out by botnets: a group of computers and/or smart devices that have been compromised by malicious automated software (a bot) so that they can be controlled remotely and without the owner’s knowledge in order to perform some collective task on behalf of the software’s creator [3].

The creators, also known as botmasters, of botnets can be individuals, groups, or national governments who act as the central command and control hub for the network of infected zombie computer systems. Botmasters have a strong economic incentive to create and spread these networks because they can be used for identity theft, mining cryptocurrency, credit card fraud, ransomware extortion, DDoS extortion, or sold or rented to the highest bidder [3, 4]. North Korea alone is estimated to have generated $2 billion in this fashion [5]. Botnets can also be used to conduct cyber espionage, secretly collecting and sending targeted information gathered through the infected network back to its owner [6]. The botmaster can use the combined computing power of all the infected devices, which typically are spread across many different countries, to whatever ends they desire with little fear of consequence because attribution is difficult to establish with a high degree of certainty, allowing states to deny their involvement with relative impunity [7].

The destructive capacity of botnets has grown significantly since the 2007 attack on Estonia as more people and especially household devices – such as fridges, thermostats, and TVs, collectively known as the Internet of Things (IoTs) – are connected to the internet each year [8]. As many as 40% of IoT devices have been reported to be part of a botnet, and by 2030, there are expected to be 125 billion IoT devices worldwide [9, 10]. However, despite the significant risk they pose, there are many important questions concerning botnets that remain unanswered [11, 12]. Why are some countries effectively managing their cyberspace while others remain riddled with botnets? Are wealthy or less-wealthy countries more vulnerable in cyberspace? Should states focus on educating their citizens about cybersecurity or should they focus on technical solutions to this problem? Are states more secure when they isolate themselves from the rest of the internet and tightly control citizens’ behavior online, or are they better off embracing digital openness and multilateral solutions to cybersecurity?

Using newly available time-series data on botnets, this paper outlines and tests the conventionally held beliefs and cybersecurity strategies at every level—individual, technical, isolationist, and multilateral. Through quantitative analysis of commonly held but largely untested beliefs about botnets and the policies intended to stop them, this study helps explain why some countries have been successful in securing their cyberspace whereas others have not. Our findings suggest that wealthier countries are actually more vulnerable than less wealthy countries; that technical solutions, including patching software, preventing spoofing, and securing servers, consistently outperform attempts to educate citizens about cybersecurity; and that countries which favor digital isolation and restrictions on internet freedom are actually less secure than those who embrace digital freedom and multilateral approaches to cybersecurity.

This study uses botnets as both an empiric metric for measuring this specific type of cyber-vulnerability as well as an important measure of general cybersecurity for two reasons. First, as previously noted, botnets pose a major threat to international cybersecurity. Although the most common use of botnets is by criminals aiming to disrupt and extort businesses, the increasing internet connectedness of sensitive government systems has led state actors to also turn to botnets for political goals, often hiring or renting botnets developed by criminal networks [13, 14]. States have used botnets to punish, silence, or disrupt their adversaries during both conventional warfare operations and peace-time. Following the attack on Estonia, Georgian government websites and communications networks were attacked in coordination with Russian ground troops in South Ossetia in 2008 [1]. Ukraine’s central election commission was “DDoS’ed” on the eve of a major election in 2019 [15]. China has used its DDoS “Great Cannon” to attack and attempt to silence international critics [16]. Voting machines in many democratic countries are susceptible as well via intermittent service disruptions that increase wait times at polling locations and decrease voter turnout [17, 18]. Used in conjunction with precinct-level polling data, these types of attacks could sway national elections or to erode confidence in the democratic process.

The second reason to study botnets is that malware infections indicate an ongoing cybersecurity challenge that shares many similar characteristics with other cyber-threats. Cybersecurity has different definitions, but generally is concerned with reducing threats to the functional integrity of computer-based systems, the confidentiality of the information stored therein, and the infrastructure they rely upon to operate as intended [19]. The greater the malware infection levels within a country, the higher the risk of sensitive information being stolen from compromised national security apparatuses or high-level phishing attempts. Further, almost all varieties of cybercrime and cyber-attacks have an element of anonymity to them. Although forensic attribution is improving, at present, it remains exceedingly difficult to prove with a high degree of certainty [7, 20, 21]. The value of anonymity in cyberspace is particularly high because it can preserve the element of surprise all the way up until the moment a cyber-attack is launched and allow for further attempts if the attack fails but anonymity is retained [22]. Botnets are the ultimate example of anonymous attacks in cyberspace and thus policies that can address them are expected to be helpful when combatting other types of cybercrime and cyber-attacks. Reducing the ability of nefarious actors to fake Internet Protocol (IP) addresses, securing servers, patching outdated software, increasing end-user education, and working on a multilateral basis to collectively secure cyberspace are all examples of anti-botnet measures that could help address other cybersecurity concerns as well.

This article proceeds as follows. The first section assesses commonly held beliefs about the different policies and approaches to cybersecurity that could affect botnet levels. This review contains three subsections outlining important ongoing debates in the field regarding which states are most vulnerable, which types of policies are most effective, and whether states are made more secure through unilateral or multilateral efforts. The second section outlines the data and methodology used to test these different approaches to cybersecurity. In the third section, the results and analysis of the study are provided. Finally, this article concludes with specific policy implications and offers both normative and treaty-based strategies to break botnets and increase cybersecurity around the world.
Cybersecurity theories and practice: How should states defend against botnets?

In the constantly evolving cybersecurity landscape, strong consensus regarding how best to fight botnets and defend against distributed cyber-attacks is hard to find. Understanding why botnet levels vary significantly from country to country is critical for developing effective policies as well as implementing them where they are most needed. Reviewing the literature yielded three major ongoing debates and each will be outlined in turn. First, we discuss botnet target selection in cyberspace, using routine activity theory with an emphasis on the number of potential targets and states’ capacity for self-defense in wealthy versus less wealthy states. Next, we outline the debate between individual-level cybersecurity approaches seeking to educate citizens about how to protect themselves online versus the technical solutions of patching software, increasing cyber hygiene, reducing IP spoofing, and establishing a national Computer Emergency Response Team (CERT), all of which can be implemented through government regulation without relying on individuals to change their behavior. Finally, we review digital isolationist strategies, such as restricting internet freedom or maintaining a “hack-back” policy for deterrence, before making the practical and legal case for why cybersecurity policies should be implemented on a multilateral basis, including through multilateral agreements such as the Council of Europe’s (CoE) Convention on Cybercrime, and how this would render all governments and individuals more secure.

Target selection in cyberspace: Are wealthy countries really more secure?

A major theory used to explain varying victimization rates between states and general target selection in cyberspace is routine activity theory. Borrowed from criminology, it contends that for victimization to occur, motivated offenders and available targets must converge in space and time and in the absence of a capable guardian [23]. Applying this theory to botnets and cyberspace, malware infections in each country should be a function of the number of available computers and IoT devices in a country (targets), the presence of botmasters worldwide (motivated offenders), and the level of cybersecurity practiced in that country (guardianship) [24]. The convergence in time and space requirements are not applicable in cyberspace as most devices are vulnerable and connected to the internet nearly all of the time. A malware-laden link may lie dormant in a spam email folder until unwittingly clicked upon, or an unpatched software vulnerability could be exploited remotely without alarming the computer’s owner. Motivated offenders are considered equally present in all countries due to the technical openness of the internet and their ability to infect computers from anywhere in the world. These offenders are assumed to be rational actors who choose their targets on the basis of potential risks and benefits [23].

The first part of routine activity theory is useful in explaining why countries with higher populations of internet users, and thus more available targets, are expected to have greater total botnet infections. Several studies have confirmed that the more available targets in a country, the higher their levels of cyber victimization [24–26]. However, the direct applicability of the capable guardian aspect of routine activity theory is less clear. Most scholars uphold the conventional wisdom that guardianship should be a factor of a country’s wealth, suggesting that citizens in higher-income states should be better able to afford the latest and most secure software and anti-virus tools [24, 27, 28]. Wealthy countries also have greater capacity for implementing cybersecurity measures, whereas lower-income states often lack the regulatory capacity, technical expertise, and funding to properly secure their cyberspace [28]. Subrahmanian et al. [27] analyzed 2 years of antivirus data from 44 countries and found a significant inverse relationship between Gross Domestic Product (GDP) per capita and botnet infections, implying that less wealthy countries were more of a threat to the global cyber ecosystem than wealthy ones. Schia [28] contends that citizens of countries with rapidly expanding internet access may also be under-informed about good online security practices, have weaker institutions, and fewer technological skills and therefore face higher risks. For this reason, some have argued that traditional development methods such as capacity building will be helpful in improving global cybersecurity [29].

However, wealthy countries may actually be targeted with greater frequency due to the perceived ability to steal more valuable information or extort more money from wealthier companies [30]. Wealthy countries may also be targeted disproportionately due to the increased processing power from higher-end computers, making them more valuable tools for use in DDoS attacks. Similarly, wealthier countries typically have faster internet connection speeds, which may also increase the disruptive capacity of DDoS attacks. However, the most important differentiating factor may be the skyrocketing numbers of IoT devices that are coming online in the homes and businesses across higher-income countries. Each new device represents a new risk and potential vulnerability, often overlooked when individuals consider their cybersecurity needs. Advocates of the conventional wisdom fire back against such claims and say that reports that find higher rates of infection in wealthy countries only do so because of the “paradox of public awareness,” claiming that such figures are not to be trusted because the wealthier a country is, the more likely it is they will detect and report malware [27]. Our study avoids this paradox by making use of data derived from third-party scanning of each country, rather than relying on self-reported statistics.

Individual education versus technical solutions: Which should states prioritize for greater cybersecurity?

There are two major clusters of research in the cybersecurity literature: those that look at human behavior to explain the misuse of technology and poor habits in cyberspace, and those seeking a technological fix to cybersecurity problems [31, 32]. Many have argued that since, ultimately, it is the devices of individual citizens that are most often infected and used in distributed cyber-attacks, educating citizens about cybersecurity practices is one of the best ways to reduce botnets and increase overall cybersecurity [11, 20, 33–35]. Botnets can spread by coaxing users to click suspicious links in emails or messaging apps, by infecting websites which then pass the bots on to unwitting visitors, or by using their combined network computing power to brute-force guess a user’s password [36]. Therefore, increasing citizen awareness of these tactics is often recommended as well as educating them on the use of firewalls and anti-virus software [3, 37]. Proponents of routine activity theory hold that this increased education will increase guardianship and thus reduce botnet infections [24].

The percentage of a country’s citizens who practice secure online behavior is expected to be higher in countries with larger Information and Communications Technology (ICT) industries, as they are assumed to have more citizens trained in basic cybersecurity practices who are more likely to employ them both in the workplace and on home devices [26]. This is the general belief and finding of many cybersecurity scholars and studies. Holt and Bossler [34] found that countries with higher levels of computer skills were better
protected than their less technologically savvy peers. Garg et al. [26] found countries with higher levels of ICT exports to be associated with fewer bots. Using higher education levels as a proxy for cybersecurity awareness, Asghari [33] found countries with higher education levels to be significantly better protected against botnets compared with countries with lower education levels. Eerten et al. [25] also found increased education to be associated with fewer infections. Survey experiment research from Gomez [38] showed that most participants were risk-averse when it comes to cyberspace, especially when wary about the past actions taken by adversaries [39]. Taking a public health approach, Rice et al. [35] also favored educating individuals, particularly on the need for “sanitation,” as applied to cyberspace infections and argued in favor of large-scale public awareness campaigns [35]. Given the outsized role of individual citizens in cybersecurity relative to other types of security, Hansen and Nissenbaum [39] rightly argue for greater inclusion and understanding of the importance of individual security practices in conversations about national security.

However, there are several problems with the emphasis on individual internet user education and applying the routine activity theory framework to cyberspace. First, even when presented with information about the dangers of risky online behavior, many individuals exhibit a resistance to making the appropriate changes necessary to better protect themselves [40]. Further, the framing of cybersecurity as a personal problem in which all the harm befalls the individual who was unguarded or careless is empirically inaccurate and additionally unhelpful for achieving positive change. The victim-blaming narrative encourages not only facilitates inaction by others but also implies a falsely narrow conception of who is really harmed by botnets. The vast majority of the harm caused by malware infections is actually external to the infected machine. Although malware could be used to steal information from the user and can slow down their system, the amount of damage that can be done is proportional to the amount of financial assets and valuable information the infected actor has [11]. For example, an individual who has little saved money to protect, such as the 40% of Americans who cannot afford a $400 emergency expense, there is little to no incentive for them to worry about cybersecurity as it is not likely to be a subject that has a major effect on their daily lives [41]. This means that there is a misalignment between the individual burden of buying, installing, updating, and running anti-virus software when much of the harm is not felt by the owner but by others [42]. For instance, an individual who uses their home computer infrequently is unlikely to notice the tell-tale slowed processing of an infected computer. As long as they can still order something online or check their bank account, they are unlikely to know that anything is wrong or seek help. However, the costs in terms of negative externalities caused by this infected computer, and millions more like it, will be felt much more strongly by others, such as the banking and financial sectors, which stand to benefit more from preventing citizens’ computers from being infected than most individuals do themselves [42].

For these reasons, some scholars support increased firm participation in cybersecurity, favoring a “poly-centric” approach and arguing that firms have the greater capacity, expertise, and fiscal incentives to tighten up security [43–45]. Companies lose trillions each year from cybercrimes [13] and, in terms of direct or centralized cyber-attacks, are particularly exposed by whichever company or vendor in their supply chain has the weakest cybersecurity defenses [46]. However, although any solution will certainly benefit from buy-in and input from the private sector, the misalignment of incentives problem remains unresolved. Despite firms having more at stake than individual internet users, when they enhance their cybersecurity against botnets this has the positive externality effect of increasing the total cybersecurity of the system, including making their competitors more secure, as now there are fewer total vulnerable computers for use in distributed attacks [47, 48]. This invokes a classic collective action problem: cybersecurity, with particular regard to the decentralized networks and attack patterns of botnets and DDoS attacks, is a non-excludable good, meaning each actor will benefit from others’ improvements in cybersecurity, thus incentivizing free-riding. As evidenced in other comparable situations, including airport security, Lojack installation, and fire-protection schemes, similar firms in competition have little incentive to band together absent regulation or another form of guarantee that other companies will invest in cybersecurity as well [46, 48]. Studies on firm-level cybersecurity investment have confirmed this suspicion that firms are incentivized to under invest and are likely to perpetuate collective insecurity [49]. Because systems are likely to fail when there is a misalignment of incentives [42], cybersecurity should instead be viewed through a government-based regulatory framework [46, 47] and with a “whole-systems” viewpoint [50]. This would allow for the implementation of widespread technical solutions and avoid reliance on under-incentivized actors to police themselves. Some technical solutions that governments should consider pursuing are: patching known weaknesses in outdated software, improving cyber hygiene by securing exploitable DDoS amplification vulnerability points, preventing the ability to use fake or spoofed IP addresses, and establishing a national CERT to quickly respond to emerging threats.

A major technical problem in need of increased regulation is that of large amounts of existing unpatched software. Unpatched software is thought to be a major source of malware infections because bots can exploit known vulnerabilities to spread to new computers by scanning the internet for the unpatched versions of software and then infecting them directly with malware [36]. An estimated 55–82 million devices are still running Windows XP, a Microsoft operating system that was phased out in 2014, and an estimated 25% of the world’s computers are still running Windows 7, which Microsoft stopped providing technical support and patching for in January 2020 [51, 52]. Outdated software like this is particularly vulnerable to botnet infections as exploitable security gaps are often found over time and then publicized online by those either seeking to fix the flaws or those seeking to abuse them. Unpatched software often remains vulnerable for long periods of time because companies have no economic incentives to fix outdated software that they no longer sell and have long since replaced. Further, companies have seen almost no legal liability when their products were used by hostile third parties to harm others [47]. One major source of unpatched software comes from software piracy as users are often too fearful to try or otherwise cannot easily update their pirated copies of software when vulnerabilities are found and need to be patched. Asghari [33] found that increased piracy was associated with increased levels of bots. Yet, some empirical studies suggest that software piracy has little to no effect on cyber-vulnerability [27] or have not been able to definitively determine its effects [25].

Another technical factor that is theorized to affect botnet levels is poor “cyber hygiene” or the number of potential vulnerabilities a country has that can be exploited to amplify a DDoS attack. Botnets can amplify the effects of their DDoS attacks through a technique known as reflection. Botmasters use their infected computers to send thousands of small fake requests to open internet servers, spoofing their own IP address to make it seem like the intended victim of the attack is the one sending requests for massively large packets of data [53, 54]. This technique allows smaller botnets to have an outsized impact, making attacks up to 179 times more powerful [55]. This
means that if a botnet acquires 100,000 computers, generally considered to be a modest size, it can amplify its attack using this vulnerability point to have the impact of a botnet with 17.9 million computers. Our conversations with cybersecurity professionals suggest that about 80–90% of all DDoS attacks use this technique.

Although a country’s level of cyber hygiene does not directly indicate whether the country has a botnet problem, it is a good measure of the government’s commitment to preventing its systems from abetting DDoS attacks [56]. Countries with more exploitable amplification vulnerabilities, such as open servers, may be thought lax and targeted by botmasters for increased expansion of their botnets. Having bots in closer proximity to amplification resources may also increase the efficacy of the botnets by reducing packet travel time, which, even though may be only microseconds, when scaled to thousands or millions of bots, this may have a more pronounced effect. In either case, reducing such vulnerabilities and the ability of infected computers to amplify their attacks substantially reduces the risks of larger scale attacks and increases the amount of bots a botnet needs to control substantially in order to be effective. This increases costs in both time and exposure to detection as they need to spread further and further, before launching their attack. Once again, the costs of securing these servers are misaligned from those feeling the harm caused by the amplified DDoS attacks, and, as such, greater regulatory enforcement or financial compensation is needed.

One of the most frequently advocated technical policies for states to implement is known as best common practice (BCP)-38. BCP-38 encourages the use of network ingress filtering, or the implementation of anti-spoofing protocols, which check incoming data packets to see if they match their assigned source IP address and dropping the traffic if the IP addresses do not match [57]. Preventing bots from using false identities is thought to greatly reduce botnets’ effectiveness because it inhibits their ability to engage in reflection attacks and amplify their effects by exploiting the lack of security on open servers [54]. This also makes botnets more vulnerable to identification and removal, meaning BCP-38 implementation greatly reduces a botnet’s survivability. If botnets are unlikely to survive after use in just one DDoS attack, their cost increases dramatically, likely reducing the total threat posed and making DDoS attacks less frequent and only available to a smaller class of wealthy patrons or patron-states. Finland has been hailed as a model state for its enforcement of BCP-38, requiring its network operators to verify the IP addresses of all traffic on their networks [57]. Elsewhere, however, absent regulation or compensation, Internet Service Providers (ISPs) often lack sufficient incentive to implement this practice because they are usually not held liable for the harm caused by malicious traffic emanating from their networks. Since inspection is costly and can significantly slow down the network’s speed, ISPs lack the incentive structure to voluntarily check traffic as this would make them less competitive than firms not conducting inspections [53, 58].

Finally, the establishment of a national CERT is widely viewed as an important step the states can take against botnets [59, 60]. CERTs have been created by many governments around the world to tackle various cyber issues from reacting to emergency situations, promoting secure technology use, helping to foster communication between actors, and identifying system vulnerabilities [60]. CERTs are likely a useful tool as Rice et al. [35] point out in their analysis of cyberspace through the lens of disease outbreak control. CERTs can play a similar role to national Centers for Disease Control, by rapidly responding to, quarantining, and dispatching emerging botnets before they can spread wildly throughout the general population. Our review of countries policies around the world indicates that only 105 countries currently have national CERTs.

**Digital isolationism versus multilateral cooperation in cyberspace: Should states build bridges or firewalls?**

Whether individual or technical cybersecurity policies are pursued, another important question remains regarding how states should interact with each other in cyberspace to increase their security. Should states attempt to wall themselves off and seek to raise their cyber defenses as high as possible or are they better off engaging and cooperating on a multilateral basis to collectively improve their cybersecurity? In the unilateral or isolationist category of approaches, we have two major policies that are claimed to be effective—tight control and monitoring of citizens’ online behavior and communications, and the hack-back deterrence policy of threatening retaliatory cyber-attacks. Multilateral approaches generally require joining international cybersecurity agreements that encourage the sharing of information and assets with other states to collectively promote better cybersecurity, including the CoE Convention on Cybercrime. These approaches are also not mutually exclusive, as some countries, such as the United Kingdom, concurrently pursue both deterrence and multilateral security strategies with partner states.

A popular unilateral approach to cybersecurity is the policy of deterrence. Some countries, such as the United States (US), profess a policy of deterring cyber-attacks by promising retaliation against anyone who would attack them. Although deterrence may play well politically, and some scholars endorse offensive capabilities as a vital component of cybersecurity [11], such tools are useless if you cannot credibly identify your attacker. Deterrence policies can only prevent DDoS attacks if attackers’ identities can be reliably determined after an attack, and this is beyond our current technical capacities to do with a high degree of certainty [7]. Although the problem of attribution may not be as bad as it was 10 years ago, forensic evidence can be spoofed and countries have an incentive to exaggerate their attack attribution cyber capabilities [21, 61]. Definitively determining the source of attacks remains a difficult issue that is often related to the political stakes involved [21]. This problem is further complicated by the conventions of international law, under which the more serious the charge levied against another state is, the higher the degree of confidence in the evidence that is needed for the charge to be upheld [61, 62].

The distributed nature of botnet attacks makes them particularly difficult to effectively deter with punitive threats. Although states’ may have a tendency toward action when responding to cyber-attacks, the decentralized nature of botnets often frustrates these efforts because botmasters are effectively hijacking the computers of unwitting third parties to carry out the attacks on their behalf. This puts an additional layer of protective concealment between themselves and the attack, making botnet use a particularly strategic choice for cyber operations in which anonymity is critical. For example, in 2019 the European Council announced its intention to deter cyber-attacks by directly sanctioning individuals involved by freezing any European assets they have and banning them from traveling to the European Union (EU) [63]. However, this is problematic not only because of the attribution challenges faced, but more critically because the computers’ owners may actually be innocent, completely unaware of their devices’ role in a botnet attack. With the chance of attribution so low and the consequences for states unclear, many may continue to find use of distributed cyber-attacks a “risk
worth taking” regardless of any state’s professed policy of hacking-back [64].

Some countries have argued that restricting internet freedom and tightly controlling information and communication flows is necessary to protect their citizens’ cybersecurity [63]. Security is often invoked by state officials, regardless of regime type, as justification for intrusive surveillance and for intercepting communications [66]. However, this policy is most heavily pursued by authoritarian countries seeking to regain lost control over their citizens. China, Iran, and Russia have argued in favor of “informational sovereignty” in an effort to nationalize their cyberspace and assert control over what their citizens can and cannot access online [67]. China’s state of the art, AI-enhanced monitoring systems allow tight control over the flow of information behind the “Great Firewall of China” [68, 69]. Russia’s new “Sovereign Internet Bill” will filter all Russian ISP traffic through special nodes controlled by the Kremlin [71]. Thailand has similar policies, particularly with regard to protecting the royal family. China also argues that the USA and other Western countries are attempting to impose a single sovereignty on the internet and cite defending their “cyber sovereignty” as a key part of ensuring their national security [68]. Through a combination of close digital surveillance and online content moderation, these states often argue that some degree of privacy and freedom need to be sacrificed in the name of security in order to protect both citizens and the state [65]. A study by Holt et al. [24] appeared to provide support for this position as they tested data on freedom and civil liberties and found democracies were associated with increased malware infections, arguing that perceived risk of botnet detection may be higher in countries with greater control over the internet leading rational botmasters to target them less frequently than more free and open states.

However, restrictions on internet freedom may actually make states less secure. Citizens seeking to circumvent these policies may resort to riskier online behavior, including downloading dodgy virtual private networks that promise the ability to bypass state content filters but actually deliver malware directly to the user’s computer [71]. Further, as Holt et al. [24] note, countries with greater freedom and civil liberties may simply appear to have increased malware infections as they are more likely to accurately report infection levels. Most importantly, no matter how much “cyber sovereignty” is gained in the attempt to control information flows within a country, such isolationist policies—short of completely cutting one’s country off from rest of the internet—will not decrease the cybersecurity threats that the country faces from botnets.

Unilateral cybersecurity strategies are flawed because the underlying internet architecture is based on a technical principle of openness, meaning a botnet anywhere in the world is an equal risk to a country’s institutions, elections, citizens, and companies as locally infected computer systems are [72]. For example, even if every American computer had advanced protections put in place and every single bot was eliminated from American territory, the US would still be nearly as vulnerable to DDoS attacks because, as our study finds, >96% of botnets are located outside the US [73]. This means the same misalignment of incentives that undermines solutions at the individual and firm levels exists at the state level. No one state has a strong enough incentive to take serious action because they would disproportionately bear the costs, while others shared equally in the benefits. The dominant strategy in such a system of anarchy is to defect, to sit idle and free-ride off of the policy moves made by others.

As such, multilateral solutions that can prevent states from free-riding are needed to most effectively fight botnets. Yet, despite many states understanding that botnets and cybersecurity are truly “board-level issues,” relatively few multilateral agreements exist between states to collectively address their insecurity [74]. Efforts to reach broad multilateral consensus by groups such as the United Nations Group of Government Experts (UN-GGE) have either led to the creation of non-binding documents, such as the 2015 UN-GGE Report, or failure to approve any form of consensus report at all, as was the case following the 2017 UN-GGE meetings [75]. The UN-GGE process breakdown, over how precisely to apply legal principles in cyberspace, has led to a multilateral fragmentation creating groups of like-minded states [75] who can more easily shape incentive structures by maintaining control over shared information and other membership benefits. The most prominent example of this type of binding multilateral agreement is the CoE Convention on Cybercrime. The convention emphasizes the need to further codify international law, delineates responsibilities to effectively manage each state’s sovereign cyberspace, and attempts to harmonize domestic cybercrime laws and procedures in order to reduce the transaction costs of international collaboration to fight cybercrime [76]. However, detractors point to issues with the convention, most notably Article 22.2 that allows states to exempt themselves from the jurisdictional rules of the treaty [77]. Domestic laws are given precedence, preventing substantive regulation at the multilateral level and rendering the convention somewhat unsatisfactory for achieving its cybersecurity goals [76]. Studies of the Convention’s effectiveness have been inconclusive, whereas Aghbari [34] found that signatories had significantly fewer bots, on average, than non-signatories, Eeten et al. [33] found that the lower average number of bots in member countries was not statistically significant.

Although this treaty falls short of the level of multilateral cooperation truly needed, it may be helpful as it attempts to harmonize domestic cybercrime laws by giving direction to states, but not imposing any legislation or rules in a top-down way [76]. Further, this convention is important because it remains the only legally binding international legislation that directly addresses cybercrime [60]. The data collection and sharing provision may help identify threats and trends earlier than states would have alone. Articles 25 and 35, which requires parties to assist to the greatest extent possible and enhances cooperation by setting up national cyber centers of contact for mutual assistance in cyber investigations, could help establish greater trust over time, enabling greater cooperation in the future [78].

When it comes to defending against botnets and DDoS attacks, the dispersed nature of the internet makes it harder for any one node, or country, in the system to understand the whole picture and quickly recognize a DDoS attack when it occurs. As the network is decentralized, so too is the traffic. It might therefore not raise any alarm bells in the countries that attacks pass through until the packets finally reach the nodes closest to the victim where all the traffic merges and inundates the target [53]. At any one point between the attacker and the victim, nothing might look too far out of the ordinary. This means that any country could essentially be complicit in either passing along a cyber-attack, participating in one unwittingly through its citizens or companies devices being infected, or abetting the DDoS attack through its open servers being exploited for amplification of the attack. States are most likely complicit through some combination of all three. Even attacks that simply pass through a state’s internet infrastructure incur legal responsibility in the transit state if that state does not make a reasonable attempt to stop the attack. Otherwise, they are in violation of the principle of nonintervention as each state is obligated under international law “not to allow knowingly its territory to be used for acts contrary to the rights of other States” [79, 80]. This international legal responsibility is orthogonal to the concept of “net
Table 1. Variable Descriptives (N = 1,769)

| Variables                  | Type or level of defense | Mean   | Standard deviation | N   | Data source               |
|----------------------------|--------------------------|--------|--------------------|-----|---------------------------|
| Average botcount           | N/A                      | 47,142 | 148,949            | 1,769 | CBL Spamhaus              |
| Internet users             | N/A                      | 15,339,385 | 56,034,133        | 1,769 | World Bank                |
| GDP per capita ($)         | N/A                      | 15,709 | 24,837             | 1,769 | World Bank                |
| ICT exports                | Composite                | 8.2%   | 9.4%               | 1,611 | ITU                       |
| Public awareness campaigns | Composite                | 48.0   | 41.0               | 571  | ITU                       |
| Unpatched software         | Composite                | 57.9%  | 21.8%              | 1,070 | Business Software Alliance |
| Cyber hygiene              | Composite                | 1,688  | 4,309              | 943  | CyberGreen                |
| CERT                       | Composite                | 36.0   | 36.2               | 571  | ITU                       |
| Spoofing rate              | Composite                | 6.8%   | 6.0%               | 198  | CAIDA                     |
| Restrictions on internet freedom | Composite       | 45.4   | 20.5               | 639  | Freedom House             |
| CoE yes                    | Composite                | 0.25   | 0.43               | 1,769 | CoE                       |
| Multilateral agreements    | Composite                | 40.6   | 43.8               | 571  | ITU                       |
| International participation| Composite                | 84.0   | 36.6               | 571  | ITU                       |
| Cybersecurity index        | Composite                | 37.3   | 27.2               | 939  | ITU                       |

neutrality” in which internet countries are meant to forward on packets regardless of their contents.

This has important implications for the sovereignty of nations and the role of international law. The United Nations General Assembly (UNGA) agreed in 2013 that the principle of sovereignty applies to cyberspace and “control over cyber infrastructure and activities within its sovereign territory” [2, 81]. The International Court of Justice ruled that although sovereignty is guaranteed to states, they have the corresponding responsibility to control all actors, including nonstate actors, within their territory and to prevent them from inflicting damages on objects or persons of other sovereign states [2, 82]. This obligation to protect the sovereignty of other states is an integral part of the principal of sovereignty [83]. As soon as a state knows, or should know, about an ongoing or impending harmful attack originating from or passing through its borders, it has the obligation to stop or prevent the attack according to its capacity to do so [84, 85]. Under this standard, less advanced states could be expected to make an attempt to stop it or at least to share information about the attack and warn the potential victims. Technologically advanced states could be expected to block the IP addresses used, to shutdown open servers, and to prevent actors in their cyberspace from being involved in DDoS attacks at all by dismantling botnets within their territory [2]. However, doing so would require monitoring of traffic by countries, governments, or both, raising difficult questions about net neutrality and first and fourth amendment rights for US citizens.

The legal and functional case for fighting botnets on a multilateral basis aside, all of these questions about botnets and cyber security remain contested—from target selection and the effects of wealth under routine activity theory, to the debate between individual education versus technical solutions, and finally to the cybersecurity implications for choosing isolationist policies such as restricting internet freedom versus engaging in multilateral cooperation. Most of these policies, and the underlying assumptions they are based on, are not empirically well-established and much of the reason for continued debate in the academic literature is due to the overall lack of robust data on botnets upon which to test these theories.

Method

Thanks to 10 years’ worth of newly available data on botnets, generously provided by Composite Blocking List (CBL) Spamhaus, we were able to substantively test the 13 theorized important variables listed in Table 1, which represents all available data regarding the policies and approaches outlined in the previous sections. Other potentially relevant variables, such as overall metrics of government effectiveness, were not included due to significant levels of collinearity, with variation inflation factors (VIFs) over 5.0, and were thereby dropped in favor of testing more actionable variables.1

Dependent variable: Average botcount

The dependent variable in this study is average botcount, which is the average number of bots found to be in a certain country on any given day during the course of that year. The botcount data used in this study comes from CBL Spamhaus, which is a nonprofit organization that tracks spam, malware, botnets, and other cyber threats [73]. CBL Spamhaus scans regularly for bots in each country in an attempt to alert users of the infection. This is more reliable than self-reported statistics because some companies, and most individuals, are often not even aware that they have been infected. Furthermore, not relying on self-reported data or disclosure of successful hackings by the countries or companies themselves is preferable because both firms and states, not wanting to appear vulnerable or rattle markets, have an incentive to keep attacks and intrusions against them to themselves or risk losing investor confidence, data-breach lawsuits, or appearing vulnerable and thus inviting further attacks. Each bot discovered by their active scanning is listed by unique IP address. Botcounts from more than 600,000 scans by Spamhaus between 2009 and 2018 were used in this study.2 Specifically, the data used were the sum of all bots found during the course of a year, divided by the total number of scans performed on each country, typically between 180 and 365 scans per year. Previous studies rely on shorter snapshots of botcounts, and this may lead to spurious conclusions as the number of bots a country has can vary significantly from month to month or even day to day due to new malware being introduced or new security flaws being exploited. Variations also occur due to the normal cycle of individuals realizing that they have been infected and then running anti-virus software. By creating a yearly average

1 The highest VIF permitted in any model was piracy rate with a 5.3, however, due to the importance of this variable, it was decided to keep it for consistency and the additional explanatory power it gave the model.

2 Botnet data for 2009 were only available from 30 June onward, and botnet data for 2018 was only available until July of that year.
Independent variables

The only true strictly control variable in this study is internet user population size, which is included to control for the number of available targets in each country. The internet users variable was generated from World Bank population and internet user percentage data. Population size was multiplied by the percentage of the population using the internet to create the combined measure. Higher numbers of internet users are expected to increase botcounts, as there is a greater availability of potential targets for botnets to infect.

The first independent variable is GDP per capita. Data for this metric was obtained from the World Bank and was calculated in current US dollars (2018). This variable was included to test the effect of wealth on cybersecurity and botnet target selection. Countries with higher levels of GDP per capita are expected to have reduced botcounts due to their increased financial and technological capacity to defend against them. Other potential metrics of a country’s wealth, such as total GDP, were excluded due to significant levels of collinearity.

To test the importance of individual user education-based solutions, two variables were included: ICT exports and public awareness campaigns. ICT exports were included as a proxy for the general cybersecurity awareness of a countries’ citizenry. Higher percentages of ICT exports are expected to reduce botcounts as a greater percentage of the population is expected to be professionally involved in cybersecurity and ostensively more aware of cybersecurity threats and best practices. Data on ICT service exports, which are the percentage of each country’s total service exports that are related to ICT services, was obtained from the World Bank. ICT exports was chosen over similar metrics, such as ICT imports, because previous studies have shown it to be most closely related to botnets [26].

The second individual-level variable is public awareness campaigns. Data on this variable comes from the International Telecommunication Union (ITU) and was included to test the effectiveness of such campaigns on a country’s botnet levels. The ITU uses survey data and secondary source confirmation to measure how widespread publicity and education campaigns about cybersecurity are within a country—including through adult education programs, public websites, nongovernmental organizations, ISPs, libraries, etc. [60]. ITU scores were converted from the ITU’s sub-metric to a 100-point percentage scale for comparability with other cybersecurity metrics.

Four independent variables were included to test the effectiveness of technical policy solutions on cybersecurity: unpatched software, cyber hygiene, CERTs, and spoofing rate. The unpatched software variable was created using software piracy rate data as a proxy measure, obtained from the 2018 Business Software Alliance (BSA) Global Software Survey. The BSA tracks the total amount of software in a country and compares it to the legally purchased amount. The unlicensed software is divided by the total software to create a piracy rate. Data was collected by the BSA every other year between 2011 and 2017 on rates of unlicensed software from 105 countries [86]. Countries with higher rates of unpatched software are expected to have higher average botcounts, as regular patching is needed to fix security flaws that are found, publicized, and exploited by botmasters.

The second technical policy variable is a measure of national cyber hygiene. Cyber hygiene refers to the number of known, exploitable vulnerabilities that can increase DDoS attack amplification risk factors within a state. Data on cyber hygiene comes from the CyberGreen Institute, a nonprofit organization that seeks to measure the health or “hygiene” of the cyber ecosystem in each country by scanning the internet for DDoS amplification vulnerabilities that can be exploited by botnets [55]. This variable was created using data from over 10 million scans by CyberGreen and was averaged per country per year from 2014 to 2018. Countries with worse levels of cyber hygiene (as indicated by higher scores on this variable) are expected to have higher average botcounts as this may indicate a lack of emphasis or capacity on cybersecurity and increased vulnerability to being targeted by botnets for growth.

The third technical variable is the presence of a national CERT. Data on this variable also comes from the ITU. The data was collected and converted in the same fashion as the public awareness campaigns variable and was included to test the effectiveness of CERTs on a countries’ botnet levels. Countries with a national CERT are expected to have lower botcounts, as they have a dedicated response team for dealing with major outbreaks and ongoing vulnerabilities.

The fourth technical variable is spoofing rate. Data on spoofing rate, or implementation of BCP-38, comes from the Center for Applied Internet Data Analysis (CAIDA). CAIDA relies on individuals to download and test the ability of countries to detect and block spoofed internet traffic [87]. As such, the original data sample was heavily unbalanced, and some countries had many scans performed, whereas others had only a few in a given year. In order to avoid falsely inflated percentages from a single or handful of scans, countries were only included if they had at least 50 spoofing tests run in a given year. This greatly reduced the sample size but protects the validity of the results in Table 2. The CAIDA figures used in this study were the percentage of successfully allowed spoofing attempts compared with the total number of attempts. Countries with higher rates of spoofing permitted are expected to have higher botcounts as the ability for bots to spoof their IP inhibits detection and increases their survivability, and further because spoofing allows for greater amplification of DDoS attack strength.

With regard to the unilateral cybersecurity policy options of deterrence and cracking down on internet freedoms, we were unfortunately only able to empirically test the latter strategy as we could not secure sufficient data on deterrence strategies. To test the effectiveness of the isolationist policy of restricting internet freedoms in the name of cybersecurity, data on restrictions on internet freedom was obtained from Freedom House’s Freedom on the Net reports. Freedom House measured restrictions on internet freedom on a scale from 0 to 100, with higher scores indicating greater restrictions on internet freedom. Freedom House considers 21 major questions and more than 100 sub questions when scoring each country in the categories of: obstacles to access (35 points), limits on content (35 points), and violations of user rights (40 points). Countries with higher restrictions on internet access are generally expected to have fewer bots due to the additional filters and greater control over internal cyberspace the country has.

Three independent variables were included to test the effects of multilateralism on cybersecurity. The first multilateralism variable is ratification of the CoE Convention on Cybercrime. All countries were dummy-coded for whether or not they have ratified the treaty [88]. Countries that have ratified the treaty are expected to benefit from the treaty provisions and collectively improve their cybersecurity, resulting in lower average botcounts than non-signatories.

The second multilateralism variable is multilateral agreements. Data on this variable also comes from the ITU, was collected and...
The ITU surveyed countries and performed confirmatory data collection and analysis to verify respondents’ answers across a wide variety of theoretically important areas [89]. Cybersecurity index scores were measured from 0 to 100, with higher scores indicating higher levels of compliance with the recommended cybersecurity policies. Countries with higher cybersecurity index scores are expected to have fewer bots as this indicates a greater overall commitment to cybersecurity across many of the domains previously discussed.

Data analysis

Generalized least squares (GLS)-based linear regression was used to analyze the potential effects of the variety of independent variables on the number of bots detected in each country in a given year. The Breusch and Pagan Lagrangian multiplier test for random effects (REs) was conducted, and we were able to reject the null hypothesis, indicating that GLS was a more appropriate model than pooled ordinary least squares for our data. GLS, RE analysis with robust standard errors “clustered” at the country-level allows for both between-country estimation and within-country estimation while standard errors “clustered” at the country-level allows for both

### Table 2 Results

| Model Variables | Botcount (1) | Botcount (2) | Botcount (3) | Botcount (4) | Botcount (5) | Botcount (6) | Botcount (7) | Botcount (8) |
|----------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| Internet users | 0.940***     | 0.917***    | 0.927***    | 1.046***    | 1.056***    | 1.108***    | 0.979***    | 0.995***    |
| CoE yes       | −0.058      | −0.066      | −0.070      | −0.063      | −0.093      | −0.101      | −0.081      | −0.066      |
| CoE yes       | 0.236**     | 0.259**     | 0.148       | 0.498***    | 0.570***    | 0.536***    | 0.333       | 0.336**     |
| CoE exports   | −0.123      | −0.127      | −0.132      | −0.103      | −0.19       | −0.191      | −0.264      | −0.208      |
| ICT exports   | −0.006      | −0.003      | −0.006      | −0.008      | −0.005      | 0.023       | 0.000       |
| Piracy rate   | 0.016***    | 0.035***    | 0.034**     | 0.024***    | 0.015**     | 0.040***    | 0.017**     | 0.058**     |
| Cyber hygiene | 0.087**     | 0.115**     | 0.062       | 0.014       | −0.003      | 0.008       | 0.013       |
| Restrictions on internet freedom | 0.003 | 0.009 | 0.016 | 0.007 | (0.007) | (0.007) | (0.007) |
| Cybersecurity index | −0.010** | (−0.003) | (−0.003) | (−0.003) | (−0.003) | (−0.003) | (−0.003) | (−0.003) |
| Multilateral agreements | −0.002** | (−0.001) | (−0.002) | (−0.002) | (−0.002) | (−0.002) | (−0.002) | (−0.002) |
| International participation | 0.003 | | | | | | |
| CERT | 0.001 | | | | | | |
| Public awareness campaigns | 0.000 | | | | | | |
| Spoofing rate | 0.020** | (−0.009) | (−0.009) | (−0.009) | (−0.009) | (−0.009) | (−0.009) | (−0.009) |
| Constant | −7.574*** | −7.333*** | −7.104*** | −13.837*** | −14.983*** | −14.254*** | −11.008*** | −11.343*** |
| Observations | 1.769 | 1.611 | 1.050 | 525 | 243 | 242 | 145 | 164 |
| Countries | 191 | 170 | 105 | 105 | 50 | 50 | 50 | 59 |
| R² | 0.742 | 0.721 | 0.647 | 0.74 | 0.773 | 0.771 | 0.765 | 0.816 |

Robust standard errors in parentheses, *P*-values are two-tailed.

*P < 0.1.

**P < 0.05.

***P < 0.01.

converted in the same fashion as previous ITU variables, and was included to test whether countries who sign on to multilateral agreements and agree to share cybersecurity information, assets, and/or expertise with other countries are better able to deal with botnets than those who do not cooperate on a multilateral basis. Countries involved in additional multilateral agreements are expected to have lower numbers of bots due to their increased collective capacity to fight them as well as the benefits of shared expertise and sharing threat information.

The third multilateralism variable is international participation. As with the variable above, the data comes from the ITU and was collected and converted in the same fashion. This variable is included to test whether countries who participate in more international and regional conferences, workshops, forums, and training events have fewer bots than countries with lower rates of international participation. Countries with more international engagement are expected to have lower numbers of bots due to increased awareness of internationally derived best practices.

The final variable, cybersecurity index, is a composite measurement of all the data from the ITU’s Global Cybersecurity Index. It was included to test the effectiveness of the totality of a country’s cybersecurity engagement across more than 20 different metrics. The ITU surveyed countries and performed confirmatory data collection and analysis to verify respondents’ answers across a wide variety of theoretically important areas [89]. Cybersecurity index scores were measured from 0 to 100, with higher scores indicating higher levels of compliance with the recommended cybersecurity policies. Countries with higher cybersecurity index scores are expected to have fewer bots as this indicates a greater overall commitment to cybersecurity across many of the domains previously discussed.
respectively. As expected for repeated observations on states, the uncorrected time-series models exhibited heteroscedasticity and first-order autocorrelation. To compensate for the intragroup correlation and heteroscedasticity, standard errors were adjusted using the Rogers method and clustered at the country level [90, 91]. Error terms were also checked for normal distributions via histograms.

Several variable transformations were necessary to facilitate the analysis. Linear regression requires the dependent variable to have a normal distribution, so average botcount needed to be log transformed to meet this assumption. Variables with extremely wide ranges or substantial outliers were identified using boxplots. Left uncorrected, these would dominate the regression due to the size effect so were subsequently log transformed to reduce potential bias. The independent and control variables that were log transformed were internet users, GDP per capita, and cyber hygiene.

All sovereign states, as recognized by the UN, were included in this study, with the only exceptions being Palau and North Korea, which lack internet user data, the critical control variable. Beyond that, a small number of country-year pairings were missing botnet data and were also excluded. Countries with some data on internet users, GDP per capita, ICT exports, piracy rate, and internet freedom had missing data points imputed using the average of prior and future scores if possible, otherwise carry forward or carry backwards techniques were used, as applicable. These techniques are considered to be a generally conservative strategy for dealing with missing data [92]. For instance, unpatched software data was only gathered every other year yet was remarkably consistent year to year, so if a country had 22% in 2011 and 24% in 2013, a score of 23% was imputed for 2012. Cyber hygiene and spoofing rates were not consistent enough year to year to justify imputation. Values were only imputed in cases with at least some reference data available. For instance, data on internet freedom was only available for 50 countries, so no imputations were attempted for the other 141 countries in this study. ITU total figures and sub-metrics were only carried forward for 2018.

Although the dependent variable data used in this study ranges from 2009 to 2018 and includes every country, many of the independent variable datasets were not complete, even after imputation, for the entire time period and often were only available for a subset of the total countries. All countries with available data were included in the study and to keep the sample sizes as large and as representative as possible, the variables were tested and added to the model iteratively, based on the number of total observations. Adding variables iteratively to the model has two primary benefits: first, it allows greater confidence in the robustness of results that are consistent across multiple different model specifications, and second, it allows for those variables with additional data to be tested against their full sample size while still ultimately including and testing all possible non-collinear variables together in the final models. Models 1–8 were iterative in this manner. Model 7 exchanges the total ITU cybersecurity index for the inclusion of four of its sub-variables. Due to the already small sample size and unbalanced nature of the spoofing rate variable, Model 8 does not have internet freedom or ITU variables as their inclusion would have resulted in a loss of 50% of the already limited sample size.

**Results**

Some of our results confirmed popular untested or undertested beliefs about botnets, whereas others directly contradicted the conventional wisdom. Surprisingly, wealthier countries actually performed worse, on average, than less wealthy states. Technical solutions robustly outperformed individual education-based approaches, with countries that had less unpatched software, fewer cyber hygiene vulnerabilities, and less IP spoofing proving significantly more secure than their peers. Restrictions on internet freedom were not shown to be a protective factor in cyberspace, and may actually make states less secure. Finally, countries participating in more multilateral cybersecurity agreements were significantly better protected against botnets than isolationist states.

Our control variable—a country's total internet users—was, unsurprisingly, the strongest and most consistent significant predictor of increased average botcounts within a country, with two to three times the predictive power of any other variable in all eight models. As such, this combined variable is recommended for use in further studies over less reliable controls such as the general population size, internet use percentage, or the number of broadband subscribers a country has. These findings are consistent with those of several previous studies [24–26].

With regard to question of how wealth affects a country's cybersecurity, our results show that, contrary to popular belief, countries with a higher GDP per capita, on average, had significantly more bots than their lower-income counterparts. Importantly, this finding suggests that higher-income countries are the best place to start targeted botnet crackdowns, rather than lower income countries, where much of the blame is often placed. Higher GDP per capita levels were significantly associated with increased botcounts in six of eight models. Both nonsignificant results, models three and seven, were positively correlated and very nearly approached significance. Overall, these findings are in conflict with those of most previous studies, likely due to our larger and more inclusive sample size. One potential explanation for this seemingly paradoxical finding is that despite greater capacity to defend against botnets, higher income countries have many more computers and IoT devices per person. Although we were able to control for the number of internet users a country has, we were not able to control for the number of devices each of those users owns, thus increasing the number of potential targets they have and increasing the likelihood they are found by the CBL Spamhaus internet scanning techniques used.

On the debate between individual-level education versus more technical approaches, our results show significant support for the increased effectiveness of technical solutions. The individual-level variables, ICT exports and public awareness campaigns, manifested no significant effect on botcounts in any of our models. Our proxy for cybersecurity awareness, ICT exports, proved to have an insignificant and somewhat inconsistent though generally negative effect on botcounts. The public awareness campaign variable was shown to have precisely zero effect on a country’s cybersecurity. Despite the null empirical finding in this study, increased education about the best practices of cybersecurity is almost certainly a positive step forward for states seeking to reduce the number of bots infecting the computers of its citizenry. However, our findings suggest that states seeking to get the greatest return on investment should instead pursue the technical solutions outlined in the following paragraphs over individual education because, whereas the “everyday security practices” of individuals are critical to the effectively securing cyberspace [39], many individuals are often resistant to changing their actual online behavior [40]. This recommendation is further supported by recent trends in botmaster behavior that are increasingly targeting cloud computing server sites for malware infections, further reducing the importance of individual user education relative to the need for more robust technical solutions. In either case, these findings concerning user education should be qualified and studied
further because, although our models used the best available proxy variable, ICT exports, which has been shown in previous studies to be the most closely related cybersecurity awareness variable to botnets [26], there remains wide variability between those who work in more technical fields and the rest of the country. Future studies should look toward creating additional metrics more targeted to capture cybersecurity education levels, perhaps relying on randomized survey experiment data in the manner discussed by Kostyuk and Wayne (2020) or by conducting randomized surveys with regard to establishing baseline figures for Gomez’s (2019) Exposure to Cyber Crime variable for each country to generate more reliable national estimates of both the prevalence of cybersecurity victimization and cybersecurity practice awareness [38, 40].

Higher rates of unpatched software, as proxied by software piracy rates, were found to be a consistent, significant predictor of increased botcounts in each of the six models it was tested in. This confirms the largely untested conventional wisdom that unpatched software is a major threat vector in cyberspace. Further research should be done on what the most prevalent unpatched software is that leads to infection and on ways to incentivize software companies to offer free, or heavily discounted, security patching for outdated software.

Poor cyber hygiene practices, as measured by the total amount of DDoS vulnerabilities a country has, was found to be a significant predictor of increased botcounts. Although significance was only reached in two of the five models in which this variable was tested, we are confident in the result because the direction of the correlation was significantly positive and the significance only dropped in the three models with much smaller sample sizes. In the case of model six, the total cybersecurity index variable likely subsumed much of the cyber hygiene variance this variable was capturing. The vulnerabilities found by CyberGreen that underlie this variable provide a tangible way to measure a country’s commitment to cybersecurity. This may lend support for theories that suggest there is selective targeting of botnet expansion in countries seen as lax on cybersecurity.

Our study could not confirm the suspected importance of having a national CERT. The nonsignificance of CERTs is surprising, yet one potential explanation is, as Choucri et al. (2014) noted, that presence of a CERT does not equate to its effectiveness [60]. Not every CERT is created equal, and there is a significant difference between having a national CERT on paper and actually having a fully funded group with the state-backing and jurisdiction needed to respond quickly to emerging threats, such as new botnets spreading rapidly throughout their country. Further research should be done to explore and test the variation of effectiveness of national CERTs, and to increase the sample size as more data becomes available.

Poor implementation of BCP-38, or network ingress filtering, as measured by higher rates of spoofing allowed, was found to be a significant predictor of increased bots. This finding in model eight confirms the previously untested assumption that cutting down on the ability of botnets to hide their identity is an effective policy tool for reducing their ability to spread and avoid detection. Although additional testing of this variable should be done as more data becomes available, further support for this technical policy can be seen in the high cybersecurity level of Finland, which requires its network operators verify the IP addresses of all traffic on their networks, and was one of the best performing countries in this study [57]. Further research should be done regarding how best to incentivize or mandate ISPs to implement network ingress filtering.

Multilateralism emerged as the clear winner in this study over isolationist strategies for cybersecurity. Although restricting internet freedom is sometimes held up as a way to combat cyberthreats, the empirical evidence does not support such a claim, and our results suggest that restricting internet freedom may actually undermine national cybersecurity. Restricting internet freedom was significantly associated with increased botnet infections in model seven and was similarly associated, though nonsignificantly, in models five and six. The finding of insignificance in models five and six alone significantly undermines claims that cracking down on internet freedom in the name of security is effective, and the significant finding in model seven directly refutes such claims. These results indicate that attempts by countries such as Russia and China to tightly control the internet are not, in fact, effective cybersecurity tools for protecting citizens, but simply repression in digital form.

Countries that exhibited greater levels of multilateral cooperation, as measured by their participation in multilateral cybersecurity agreements and efforts to share information, expertise, and assets with other countries, were significantly better protected against botnets than their less cooperative peers. Of the three multilateralism metrics, only the multilateral agreements variable reached the level of significance, and further testing of these ITU sub-metrics is recommended as new data becomes available. Our results suggest that the CoE Convention on Cybercrime is having a modestly beneficial impact on cybersecurity and support earlier findings by Eeten et al. [33] and Asghari [33]. Ratification of the convention had a protective effect against botnets in all eight models, yet only approached significance (above the 90% confidence level) in two of these models. These results indicate that this policy measure, on its own, may be helpful but not sufficient and that further strengthening of this convention may be required if it is to have its intended effect.

Changing Article 22.2, which dramatically undermines the treaty by allowing states to exempt themselves from the jurisdictional rules, as well as increasing provisions for information and expertise sharing, would likely be a good place to start.

Our variable on international participation was not significantly associated with botnets and this may be due to the limited distribution of the variable scoring as the average participation rate among states was 84%. This suggests that simply showing up to major international cybersecurity conventions, forums, workshops, etc. is not enough to enhance a state’s security in cyberspace, especially if the best practices learned are not implemented upon returning.

The composite total metric for cybersecurity best practices, as measured by the ITU’s cybersecurity index scores, was found to be a significant predictor of decreased bots. This provides some empirical support for the wide variety of policies, tools, and approaches they prescribe, from greater multilateral cooperation, to capacity building, to setting a national cyber strategy, and strengthening public-private partnerships.

Discussion
This study finds that wealthier countries are more vulnerable than less wealthy countries; that technical solutions, including patching software, preventing spoofing, and securing servers, consistently outperform attempts to educate citizens about cybersecurity; and that countries which favor digital isolation and restrictions on internet freedom are actually less secure than those who embrace digital freedom and multilateral approaches to cybersecurity. Due to the global, decentralized nature of this threat, as well as the legal obligations of states under international law to prevent their cyberspace from being used to attack others, this study recommends the creation of stronger normative agreements to implement empirically determined best practices as well as the creation of stronger legally
binding multilateral cybersecurity agreements to fight botnets around the world.

Of these technical issues, remedying unpatched software and implementing BCP-38 are urged as the most pressing. States should develop policies to promote patching of known software vulnerabilities within a short timeframe. Creating incentives to provide patches to pirated versions of software should also be considered and these security-only patches should be kept separate from product feature upgrades [33]. This will allow companies to keep their newest and best products in the current market incentive structure while securing their older products against exploitation. Governments should also regulate or incentivize the implementation of network ingress filtering on a widespread basis in order to cripple the ability of botnets to evade detection and amplify their attacks. Cutting down on IP spoofing has the additional benefit of reducing DDoS attack potency on top of an increased ability to detect and remove bots. This combined effect will go a long way in securing cyberspace. States should create incentives for compliance, including compensation for increased costs, as a cost-effective way to increase global cybersecurity. While implementation may seem somewhat expensive during the transition period, this will prove far cheaper than the long-term system-wide losses incurred by botnets and DDoS attacks.

Our results show that the conventional wisdom from routine activity theory, holding that lower income countries are less secure due to their lower capacity to protect their cyberspace, is misinformed. The reality is that the vast majority of countries, especially the wealthy ones with their skyrocketing numbers of new IoT devices, are woefully unprepared and relatively insecure. International efforts to fight botnets should be focused on higher-income countries, who unwittingly pose a much greater threat to global cybersecurity through DDoS complicity than lower-income countries do. Although higher-income countries account for the majority of botnets at present, as lower income states become increasingly connected, cybersecurity technology and expertise transfer to the global south will become increasingly important. The UNGA Resolution on the Creation of a Global Culture of Cyber Security affirmed this need, and this resolution could form the basis for greater future multilateral cooperation in cyberspace [93].

As China looks to start changing the rules of cyberspace, especially through the building of its 5G network and laying the fiber optic cables for the “Digital Silk Road,” which has already reached 50 of 64 countries as part of the Belt and Road Initiative, major efforts to counter their false narrative concerning reclaiming sovereignty and security at the expense of privacy and freedom must be countered [94]. Not only are such efforts to crack down on internet freedom ineffective, they are also counterproductive from a security standpoint, as they likely force citizens to use programs they do not fully understand as they attempt to circumvent national content filters.

Developing cyber norms will be an important part of global cybersecurity. While more significant institutionalized international cooperation in cyberspace is what is truly needed to combat botnets, this level of cooperation remains exceedingly difficult under the current global governance structure and growing populist backlash against international institutions. Yet, even without an overarching institution in place to enforce action on this issue, progress can be made on a peer-to-peer basis [95] as the current structure of nonexclusive security externalities encourages free-riding only insofar as it is deemed socially acceptable [48]. The Chair of the Open-Ended Working Group on ICTs, a committee created by the UNGA in 2018, noted that the areas of consensus among the Member States comprise roughly 80% of the cybersecurity issues raised and the divisive issues comprised only the remaining 20% [96]. Thus, strengthening cyber norms in those areas of common concern, such as what the Association of Southeast Asian Nations has done with regard to transnational cybercrime [97], and the use of “naming and shaming” techniques to encourage good behavior may be a useful stop-gap technique until sufficient global governance structures can be put in place to functionally regulate and secure cyberspace [98]. Broadly worded codes of conduct and rules of behavior have the benefit of allowing a coalition to be as wide and inclusive as possible and allow enough room for states to not feel pressured or constrained in a threatening way [99]. The establishment of stronger norms via creation of a taboo against targeting civilians, harboring cybercriminals, and attacks that cross the “use of force” threshold could be effective at curbing some of the worst attacks [98]. Countries should also push for the regulation and enforcement of anti-spoofing protocols as the default and norm for ISPs, as Finland has already done, and those who do not should be labeled and called out for their deviant behavior.

Normative development can be catalyzed by the adoption and championship of these policies by norm entrepreneurs and model states [100]. Governments with good reputations, such as Switzerland with its reputation for neutrality, or impartial global CERTs could be helpful in bridging the gap between skeptical states. Naming and shaming countries that are not doing enough to uphold their sovereign responsibilities to prevent their infrastructure, servers, and citizens from being unwittingly used to carry out DDoS attacks could be helpful for norm development and to police defectors. Both the CoE and the ITU maintain databases on national legislation, combining their tracking with the ongoing work of Cybergreen, Spamhaus, and CAIDA to track botnets, cyber hygiene, and BCP-38 implementation, the members of the emerging cybersecurity epistemic community could reach the level of consensus needed to bring sufficient international pressure on states to change their behavior and work collectively on this issue.

Distributed attacks can be best countered with distributed defenses. Pooling server resources via load balancing to reduce the down-time of companies under attack by lending unused servers to those in need during a DDoS attack and then reciprocating when necessary could be a useful strategy and thereby reduce the incentives for such attacks in the first place. Although conventional deterrence is not readily transferable to the cyber realm [101], coordinated responses to shape traffic and flex bandwidth to mitigate the effectiveness of cyber-attacks could deter some would-be attackers by increasing the costs needed to carry out the attacks and reducing their efficacy below whatever threshold of disruption might be considered a “successful” attack [102]. Pooling information and expertise is just as important, as shown by the significance of the multilateral agreements variable. Keeping informed on the most up-to-date information on system vulnerabilities, secure coding practices, data on attacks, and malicious IPs/websites could go a long way in improving our collective cybersecurity. Ideally, information sharing should be automated, so that the speed of responses can be increased to rival the speed of changing offensive cyber capabilities.

Due to the global, decentralized nature of these attacks, this study recommends the creation of stronger legally binding multilateral cybersecurity agreements to implement technical policies in alignment with these findings. In tandem, it recommends a multilateral treaty explicitly prohibiting the use of DDoS attacks outside of conventional conflicts, with a focus on ensuring that the laws of armed conflict apply in the cyber realm and with particular regard for noncombatants. This treaty should enshrine special protections
for hospitals and critical infrastructure, including the electric grid and voting systems. Additionally, provisions requiring assistance in fighting attacks originating from inside a sovereign state’s territory during peace time would be helpful and would allow states to judge the originating state’s level of assistance to indicate their level of complicity in the attack [8]. Calls have been made already by industry leaders for a “digital Geneva Convention” or a world organization for cybersecurity, in the spirit of the World Health Organization [103]. Another potential effective method would be to change the CoE Convention on Cybercrime to allow universal jurisdiction instead of giving deferential preference to domestic laws [76]. This would represent a drastic shift in not only cybersecurity enforcement but in international law generally. The functional level of the internet is truly global, so for cyber policies to be most effective, they should be implemented at the global level.

States will remain the most important actors in cybersecurity. Although state-based treaty approaches have been justly criticized for being too top-down for cyberspace, and effective policy solutions need to be multi-stakeholder, ultimately states are still the principle actor in cybersecurity [2]. They are also the only actors that can be held accountable under international law, so solutions to this issue must start with them. States have an obligation under international law to prevent potentially harmful attacks from being carried out within or through their territory, and states are legally bound to prevent such activities from occurring in their cyberspace [84]. If a state was aware, or should have been aware, they must take all reasonable measures—according to their capacity—to stop such attacks [84].

The overall resilience of the global cyber system is dependent on the security of its weakest links. Our collective fates have become physically intertwined by fiber optic cables. Therefore, effective solutions need to be as inclusive as possible on the global scale. The development and strengthening of cyber norms could be a useful measure, while institutional solutions are worked out and the trust needed to establish them is built. Many countries are skeptical of the US, and its unwillingness to enter international agreements in cyberspace feeds into this narrative [8]. The US should drop its unwillingness to negotiate and follow the EU’s example as institutions need to be built which are more credible and impartial than national government agencies. Instead of working through the major powers directly, Choucri et al. [61] have suggested that the ITU could be a useful vessel for international cooperation because it has an institutional mandate to standardize and better facilitate communications systems between UN Member States as well as a reputation for technical neutrality. India has already supported a similar proposal for the ITU to take greater control of governing cyberspace on the global scale, and this proposal could serve as a basis for coalition building and ultimately breaking botnets once and for all.

Acknowledgements

The authors are grateful for the support provided by the Global Resilience Institute at Northeastern University, the research assistance provided by Akash Patel, and the critical analysis and feedback of three anonymous reviewers. The authors are also grateful for generous provision of data from CBL Spamhaus, CAIDA, Cybergreen, and the ITU.

Conflict of interest statement. The authors declare no conflict of interest or specific sources of funding for this research. Financial support for the open access publication was generously provided by The William and Flora Hewlett Foundation.

References

1. Reich P, Weinstein S, Wild C, Cahanlong A. Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents – and the Dilemma of Anonymity. European Journal of Law and Technology 2010;1:21–58.
2. Cho Y, Chung J. Bring the State Back In: Conflict and Cooperation among States in Cybersecurity. Pacific Focus 2017;32:290–314.
3. Zargar ST, Joshij T, Tipper D. A Survey of Defense Mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE Commun Surv Tutorials 2013;15:2046–69.
4. Negash N, Che X. An Overview of Modern Botnets. Inf Secur J 2015;24:127–32.
5. Nichols M. North Korea took $2 Billion in Cyberattacks to Fund Weapons Program: U.N. Report. Reuters 2019.
6. Wangen G. The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism. Inf 2015;6:183–211.
7. Schulke M. The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty. Perspect Pol 2018;16:954–68.
8. Knake R. Internet Governance in an Age of Cyber Insecurity. New York, NY: Council on Foreign Relations, 2010.
9. Lohachab A, Karambir B. Critical Analysis of DDoS—an Emerging Security Threat over IoT Networks. J Commun Inf Networks 2018;3:57–78.
10. Howell J. Number of Connected IoT Devices will Surge to 125 Billion by 2030. HIS Technol London, United Kingdom, 2017. https://news.ihsmarkit.com/pvreview/release_only/slug/number-connected-iot-devices-will-surge-125-billion-2030-ihsmarkit-says (1 June 2018, date last accessed).
11. Kleinberg H. Building a Theoretical Basis for Cyber Security Best Practices. Ann Master Sci Comput Sci Inf Syst UNC Wilmingt 2015;9:2–103.
12. Stevens T. Global Cybersecurity: New Directions in Theory and Methods. PoliGov 2018:6:1–4.
13. Morgan S. Cybersecurity Ventures 2016 Annual Cybercrime Report. Northport, NY, 2018.
14. Khan FU. States Rather than Criminals Pose a Greater Threat to Global Cyber Security: A Critical Analysis. Strateg Stud 2011;31:91–108.
15. Hanson F, O’Connor S, Walker M, Courtous L. Hacking Democracies: Cataloguing Cyber-enabled Attacks on Elections. Asiat Strategy Policy Inst, Report No. 16, Barton, Australia, 2019. https://s3-ap-southeast-2.amazonaws.com/ad-asp/2019-05/Hacking%20democracies.pdf (1 February 2020, date last accessed).
16. Marczak B, Weaver N, Dalek J, et al. China’s Great Cannon. Research Brief, The Citizen Lab, University of Toronto, Toronto, Canada, 2013.
17. Culnane C, Elidridge M, Essex A, Teague V. Trust Implications of DDoS Protection in Online Elections. Cryptogr Secur 2017; 10615 LNCS: 127-145. doi:10.1007/978-3-319-68687-5_8
18. O’Flaherty K. Expert Warns That This Common Cyber-Attack Could Hit The Midterm Elections. Forbes 2018.
19. Adams S, Brokx M, Dalla Corte L, et al. The Governance of Cybersecurity: A Comparative Quick Scan of Approaches in Canada, Estonia, Germany, The Netherlands and the UK. Tilburg University, Tilburg, 2015.
20. Desnoyers S. The Challenges of Cybercrime for International Law Enforcement, ProQuest, Ann Arbor, Michigan, 2013.
21. Reiter T, Buchanan B. Attributing Cyber-attacks. J Strateg Stud 2015;38:4–37.
22. Brantly AF. The Decision to Attack: Military and Intelligence Cyber Decision-Making, Georgia Press, Georgia, 2016.
23. Felson M, Cohen LE. Human Ecology and Crime: A Routine Activity Approach. Hum Ecol 1980;8:389–406.
24. Holt TJ, Burress GW, Bossler AM. Assessing the Macro-level Correlates of Malware Infections using a Routine Activities Framework. Int J Offender Thy Comp Crime 2018;6:2:1720–41.
25. Eeten M, Bauer JM, Asghari H, Tabatabaee S, Rand D. The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis based on Spam Data. Work Econ Inf Secur 2010;5:1–31.
26. Garg V, Koster T, Camp JJ. Cross-country Analysis of Spambots. EURASIP J Inf Secur 2013;1:3:1–13.
27. Subrahmanian VS, Ovrelinne M, Dumitras T, Prakash BA. The Global Cyber-Vulnerability Report. Cham: Springer International Publishing, 2015.
76. Stevens SR. Internet War Crimes Tribunals and Security in an Interconnected World. Transnatl Law Contemp Probl 2009;18: 657–720.
77. Council of Europe. Convention on Cybercrime. Eur Treaty Ser 2009;2: 1–21.
78. Adrian A. Could a small town in Romania bring Australia to its knees? Not if they accede to the EU convention on cybercrime. J Int Commer Law Technol 2012;7:328–38.
79. ICJ T. Latest developments Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania) International Court of Justice, The Hague, Netherlands1949.
80. ICJ T. International Court of Justice: Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America); Merits, Judgement, The Hague, Netherlands, 1986.
81. United Nations General Assembly Group of Governmental Experts. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, New York, 2013.
82. ICJ T. International Court of Justics: Judgments: Pulp Mills on the River Uruguay (Argentina v. Uruguay), The Hague, Netherlands 2010.
83. The Permanent Court of International Justice. Reports of International Arbitral Awards: Island of Palmas Case: (Netherlands v. USA), The Hague, Netherlands, 1928.
84. Couzigou I. Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations. Int Rev Law Comput Technol 2018;32:37–57.
85. ICJ T. International Court of Justice: Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Monte Negro), The Hague, Netherlands, 2007.
86. BSA. Software Management: Security Imperative, Business Opportunity, Business Software Alliance Global Software Survey, 2018. https://gs.sbsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf (1 June 2018, date last accessed).
87. CAIDA. Data Collection, Curation and Sharing. The Center for Applied Internet Data Analysis, 2018. https://www.caida.org/data/ (1 June 2018, date last accessed)
88. CoE. Chart of Signatures and Ratifications of Treaty 185. Council of Europe Convention on Cybercrime 2018, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (1 June 2018, date last accessed).
89. ITU. Global Cybersecurity Index 2015/16 Questionnaire Guide, International Telecommunication Union. 2015.
90. Hoechle D. Robust Standard Errors for Panel Regressions with Cross-sectional Dependence, Stata J. 2007;3:281–312.
91. stata Xtregr—Fixed-, Between-, and Random-effects and Population-averaged Linear Models,2020. Stata.com
92. Gelman A, Hill J. Missing-data imputation. In: Data Analysis Using Regression and Multilevel/Hierarchical Models. Cambridge: Cambridge University Press, 2006, 529–44.
93. UNGA. Resolution on the Creation of a Global Culture of Cyber Security, 57th Session, United Nations General Assembly, New York. 2003.
94. Segal A. When China Rules the Web. Foreign Aff 2018.
95. Ostrom E. Governing the Commons: The Evolution of Institutions for Collective Action. Cambridge, UK: Cambridge University Press, 1990.
96. Korzak E. OEWG on Cybersecurity: First week of the open-ended working group at the UN in New York/Zurich Hub for Ethics and Technology, 2019.
97. TranDai C, Gomez MA. Challenges and Opportunities for Cyber Norms in ASEAN. J Cyber Policy, 2018; 3;2:217–235
98. Nye JS. Normative Restraints on Cyber Conflict, Cyber Security Project, Belfer Center for Science and International Affairs, 2017.
99. Saran S. Striving for an International Consensus on Cyber Security: Lessons from the 20th Century. Glob Policy 2016;7:93–95.
100. Finnemore M, Hollis DB. Constructing Norms for Global Cybersecurity. Am J Int Law 2016;110:425–79.
101. Clark R, Knake R. Cyber War: The Next Threat to National Security and What to Do about It. New York: Harper Collins, 2010.
102. Nye JS. Deterrence and Dissuasion in Cyberspace. International Security 2017;41:44–71.
103. Koch M, Riedel D. Hacker Soldiers: Germany could dispatch armed forces in response to cyberattacks. Handelsblatt Today 2018.