# Requisites for Successful Cyber Deterrence:
# Multi-actor Network of Great Powers, Smaller States, and Non-State Actors[1]

## Abstract

This study analyzes the successful conditions and inner-working mechanisms for deterrence through multi-actor systems. In doing so, the paper outlines how involved actors distinctively contribute to, and profit from, participating in multi-actor systems. Considering the relevance of hard power capabilities, power diffusion, and normative reputations in cyberspace, every involved actor has its competitive edge and, in turn, augments its 'hard and soft power' capability by joining forces. Great powers, as the most powerful actors, use their superiority in offensive operations, defense networks, attributive skills, and traditional security measures to underpin the deterrence framework. Meanwhile, other states with less military power and non-state entities supplement the system by providing *de facto* response mechanisms against asymmetrical "gray zone" threats that take advantage of asymmetries in cyberspace. Given the importance of reputation and credibility in the internet era, users around the world collectively raise the moral and financial cost of attack for adversaries entangled within the global economy. Ultimately, multilateral coalitions ensure their long-term viability by providing incentives for membership and shifting the decision matrix of actors toward joining the institution.

## I. Introduction

Collective action happens when relevant stakeholders perceive mutually beneficial solutions to be more profitable or risk-averse than choosing not to cooperate. Without significant advantages, multilateral systems lack merit over unilateral actions and merely consist of perfunctory participation by members. Yet international institutions have long failed to provide clear incentives for engagement. Great powers remain discontented about contributing a disproportionate amount of financial resources to sustain "aimless" multilateral organizations and have shifted their priority to unilateralism.[2] Likewise, other states question the effectiveness of regimes as they lack enforceability and become constrained within the international distribution of power.[3] Such a dynamic intensified under the Trump administration and, while the United States (U.S.) declared a return to global partnerships under President Biden, the underlying motive was to check China's rising power. In essence, multilateralism has lost its true purpose.

Considering these challenges, how might the circumstances in cyberspace differ and compel stakeholders to partake in a security coalition? Over the past decade, multiple organizations such as the International Telecommunication Union (ITU), Internet Corporation for Assigned Names and Numbers (ICANN) and the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) have sought to provide a governance model for global networks. In 2020, the U.S. launched the Clean Network Initiative,

[1] This paper observed The Chicago Manual of Style.

[2] Case in point, the U.S. withdrew from "unfair" international agreements including the Trans-Pacific Partnership and the Paris Climate Accord under President Donald Trump.

[3] The United Nations Security Council (UNSC), for instance, has long been criticized for valuing the strategic needs of the five permanent members over "any truly human concern" in humanitarian intervention cases (Rajan, 3). While the UNSC eagerly protected Kuwait under Iraqi occupation due to a vested interest in oil resources, they lacked "enthusiasm to prevent killings in Rwanda."

inviting more than 50 nations and 180 telecommunication companies to comply with "internationally accepted" digital trust standards and implement the use of clean technology.[4] Although still at its inception, the initiative has succeeded in undermining Chinese information technology (IT) vendors that pose cybersecurity risks: Huawei contracts abroad shrunk from 91 to a dozen in less than a year.[5] As such, current frameworks divert from the spirit of collaboration and focus on punishing others based on the political agenda of great powers.

While existing studies in cyberspace spot potential areas for international cooperation, they remain skeptical about the establishment and sustainability of multi-actor cybernetworks. Despite the need for global coordination, Nye (2011) underlines how cooperative frameworks "remain weak" with nations concentrating on the "zero-sum rather than the positive-sum aspect."[6] Refuting the idealized myth of global governance, Min (2017) uncovers how cyber coalitions mainly serve as a tool for super powers and fail to represent the majority of state and non-state actors. By the same token, Kim (2014) highlights the hegemonic competition between America's multi-stakeholder and China's inter-governmental model and subsequently depicts the role of middle power diplomacy amid such structural conditions. Urgessa (2020) argues how cybersecurity coalitions will not achieve significant progress due to global cooperation being in a "state of gridlock."[7] As a whole, previous research criticizes the reality of great power-centered multi-actor systems and justifies the need for increased middle and smaller power participation.

In addressing the literature gap, this study examines the effectiveness and sustainability of cyber deterrence by multilateralism.[8] Given the relevance of hard power capabilities, power diffusion and normative reputations in cyberspace, every involved actor has its competitive edge and, in turn, augments its hard and soft power capability through combining forces. The paper argues that while great powers underpin the deterrence framework based on their unrivaled military and economic resources, other state and non-state actors complement the system by providing applicable response mechanisms against asymmetrical "gray zone" threats arising from low-cost malware. Ultimately, multi-actor networks not only elevate the cost of attack for hostile actors but also incentivize its participants through strengthening dissuasion by denial, punishment, entanglement and norms compared to unilateral cases.

## II. Characteristics and Significance of Cyber Threats

Referred to as the fifth operational realm, cyberspace consists of both commonalities and differences with the conventional territorial (land, sea, air) spheres. Despite the increasing societal dependence on electronic devices and virtual settings, physical infrastructure and geographical space still matter the most in international affairs. As evidenced by the ongoing global pandemic and territorial disputes, the world has yet to achieve the complete virtualization of daily activities and inter-state

[4] United States Department of State, "The Clean Network," January 17, 2021.

[5] Peter Coy, "U.S. Policy on China May Move from 'America First' to America & Co," Bloomberg, December 9, 2020.

[6] Joseph Nye, "Nuclear Lessons for Cybersecurity?," *Strategic Studies Quarterly* 5, no. 4 (2011): pp. 18-38.

[7] Urgessa, Worku Gedefa. "Multilateral cybersecurity governance: Divergent conceptualizations and its origin." *Comput. Law Secur. Rev.* 36 (2020).

[8] Following its literal definition ("many-sided"), the word "multilateral" will be defined as comprising both state and non-state entities and hence used interchangeably with the term "multi-actor" throughout the paper.

relationships. Conversely, amidst the growing connectivity to digital networks, the cyber domain has diffused power to multiple actors and challenged the "primacy of states" as the exclusive source of power.[9] The packet-switched networks were initially devised for military purposes by the U.S. Department of Defense; they later became commercialized by corporations and expanded into a worldwide network known as the Internet.[10] The growing global influence of social media and search engine platforms also signals the importance of soft power measures, including normative reputations within the realm.

Resembling the domain's complex characteristics, attacks in cyberspace have emerged as asymmetrical threats to the privacy of citizens, intellectual property of companies and functioning of national infrastructures. In particular, the universalization of technology has reconfigured the power distribution within the international system and empowered traditionally weaker states, private entities and rogue organizations. Unlike conventional weapons, which require significant material and human resources, cyber attacks have low entrance barriers as anyone with a connected device can generate malicious code. Accordingly, the existing power dynamics continue to be undermined by the greater participation of actors that "fall outside of traditional deterrence frameworks." A cyber espionage network, Ghost Net, corrupted "1,295 computers in 103 countries, of which 30 percent were high-value governmental targets."[11] North Korean hackers utilized the infamous Wannacry ransomware to target the public and private sectors of over 150 nations. Such instances exemplify how cyber weapons "reduce power differentials" by serving as an economical choice for smaller state and non-state entities.[12] In short, cyber attacks occur frequently, target all levels of society and, if successful, entail significant political and financial costs.

The anonymity and multiplicity of actors further cause attribution problems for targeted entities. Contrary to missiles and nuclear weapons that leave traceable markers, actors in the cyber domain avoid accountability through sophisticated deception methods such as hiding their identity behind proxy servers. Even with the presence of forensic technology, pinpointing the origin of an attack requires significant effort as more than half the world's population is connected to the Internet as of 2018.[13] For instance, although initially attributed to Russia, the JPMorgan Chase data breach was executed by two individuals living in Moscow and Tel-Aviv.[14] As such, states face difficulty in pinpointing responsible actors, connecting individual operators to governments that fund their malevolent actions, and eventually determining the appropriate course of retaliation.

[9] Anthony Craig and Brandon Valeriano, "Realism and Cyber Conflict: Security in the Digital Age," *E-International Relations*, 2018, pp. 1-11, 4.

[10] Breno Pauli Medeiros and Luiz Rogeiro Franco Goldoni, "The Fundamental Conceptual Trinity of Cyberspace," *Contexto International* 42, no. 1 (2020): pp. 31-48, 41.

[11] Joseph Nye, *Cyber Power* (Cambridge, MA: Harvard Kennedy School Belfer Center for Science and International Affairs, 2010), 9.

[12] Ibid., 1.

[13] Max Roser, Hannah Ritchie, and Esteban Ortiz-Ospina, "Internet," Our World in Data, July 14, 2015.

[14] Joseph Nye, *Cyber Power* (Cambridge, MA: Harvard Kennedy School Belfer Center for Science and International Affairs, 2010), 52.

## III. Conditions for Successful Multilateral Deterrence

With regards to growing cyber threats, sovereign states and non-state organizations alike have tried to devise deterrence methods that diminish the likelihood of aggression from adversaries. Nye (2017) identifies four key mechanisms that constrain cyber risks. Alongside classical dissuasion methods including credible threats through punishment and denial by defense, political factors such as entanglement and normative taboos "reduce adverse actions" in cyberspace.[15] The major forms of deterrence, although imperfect individually, complement one another in countering cyber attacks. Given that each mechanism has its strengths, weaknesses, and main target group, combining different cyber deterrence instruments will produce a synergy effect and influence "hostile actors' perception of the costs and benefits of particular actions."[16]

How can multilateralism bring together dissimilar methods to better avert conflict and intrusion in cyberspace? In answering such a question, one must first specify the requisites for successful cyber deterrence. Adapting definitions from existing studies, conditions for traditional nuclear deterrence include the "defender's capabilities, the credibility of the threat, and relaying the threat message to the challenger."[17] Consistent with the case for territorial domains, actors must develop strong offensive and defense systems and employ these reinforced hard power measures to discourage potential adversaries. However, the nuclear analogy involving "massive retaliation" does not perfectly suit the needs of entities in cyberspace. In 2012, malware dispatched by Iranian forces damaged 30,000 computers of the Saudi Aramco Corporation and paralyzed the corporate's communication service and internal network.[18] Yet, as these forms of attack qualified as "malicious but bloodless acts," Iran took advantage of the fact that armed weapons will not be deployed and continued pursuing such low-level intrusions.[19] In addition to satisfying conventional requirements, efficient cyber dissuasion methods must hence have *actual* consequences on the challenger.

Grounded on such conceptualization, subsequent chapters elucidate how involved actors distinctively contribute to, and benefit from, participating in multi-actor systems. As the strongest actors, great powers utilize their superiority in offensive operations, defense networks, attributive skills, and traditional security measures to prevent armed-level cyber attacks on coalition members. On the other hand, smaller state and non-state actors substantiate the existing framework by enabling *de facto* deterrence against gray zone threats that exploit the asymmetries in cyberspace. States with less military capabilities contribute to collective defense through custom-made strategies against specific opponents. Private corporations and skilled individuals protect the public by distributing patches and attribution methods. Collectively, the multiplicity of participants in multilateralism raises the financial and moral cost of attack for adversaries entangled within the global economy. It should be noted that the aforementioned

[15] Ibid., 54.
[16] Ibid., 62
[17] Amir Lupovici, "Cyber Warfare and Deterrence; Trends and Challenges in Research," Military and Strategic Affairs 3, no. 3 (2011): pp. 49-62, 50.
[18] "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back (Published 2012)," The New York Times, 2021, .
[19] Sean Lawson, "Putting the 'WAR' IN Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United State," *First Monday* 17, no. 7 (February 2012), https://doi.org/10.5210/fm.v17i7.3848.

processes are not a series of independent actions, but rather an interactive model that builds upon the success of one another.

## IV. Great Powers: Establishing the Framework for Credible Deterrence

Cyberspace operates under realist constraints whereby great powers have a significant advantage in monetary capabilities to pursue their goals. According to the Belfer Center's index measurement in 2020, the permanent five members (P5) of the United Nations Security Council (i.e., China, France, Russia, the U.K., and the U.S.) all rank within the "top six" for nations[20] with the strongest cyber power.[21] Reflective of such hierarchy, great powers define the cyber domain as their top priority and make significant investments to "subsidize infrastructure, computer education and protection of intellectual property."[22] The United States, for instance, has allocated $9.8 billion[23] in cybersecurity for its national budget for 2022, with $750 million being used to restore agencies "affected by recent cyber incidents."[24] Characteristically, President Joe Biden has increased funds for the modernization of network defenses such as "improving logging practices [and] deploying multi-factor authentication and encryption technologies."[25] Competing alongside the United States, China has accelerated its funding into the research and development of digital space and the U.K. achieved a "new record year for cybersecurity investment" in 2020.[26] Even non-state actors, symbolic of power diffusion, have capability gaps depending on their home country status: most of the successful multinational IT firms have their headquarters in great power nations and receive funding from their respective governments to empower security networks. In sum, despite the increasing number of smaller states and non-state entities, governments with superior economic and technological forces remain as the strongest actors in cyberspace.

Based on their financial and military prowess, great powers could provide extended deterrence against cyber threats for their security allies. Extended deterrence refers to the military capabilities of a given nation to deter potential attacks on allies. Case in point, nuclear weapons states continue to offer security umbrellas and ensure a nuclear response for enemy attacks against allied nations. In the multilateral context, cornerstone clauses such as Article 5 of NATO define an "attack against one Ally is an attack against all Allies" and emphasize the importance of collective security and interdependence. Transitioning to cyberspace, major states could lead multi-actor coalitions by 'hard power' and establish frameworks for collective deterrence based on their coercive strength.

[20] The U.S. and China lead the ranking followed by the U.K. and Russia. Outside the UNSC nations, Netherlands is placed fifth above France, while Germany, Canada, Japan and Australia comprise the remaining list for top ten (National Cyber Power Index 2020, pg. 8).

[21] Julia Voo et al., *National Cyber Power Index 2020* (Cambridge , MA: Harvard Kennedy School Belfer Center for Science and International Affairs, 2020).

[22] Nye, "Cyber Power," 9.

[23] To put into perspective, the $9.8 billion investment into a single security sector is greater than the gross domestic product (GDP) of more than 50 nations (Worldometers, 2017).

[24] Office of Management and Budget, *Budget of the U.S. Government* (Washington: The White House, 2021), 32.

[25] The White House Briefing Room, "The United States Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," The White House, July 19, 2021.

[26] Julia Voo et al., National Cyber Power Index 2020, 40.

### *1. Offensive Operations*

Contrary to claims that the most powerful nations underperform against weaker actors, great powers lead the cyber offense and can underpin their allies' deterrent threats against adversaries. Diffusion of power does not entail equalization of power. The international system consists of self-interested states that struggle to obtain relative power over each other. Consequently, operational domains such as land, sea, air, and space serve as arenas that rank states from greatest to weakest; the case for the cyber realm is no different. While small states and non-state actors utilize low-cost malware to harm the most developed nations, the capacity and impact of cyber operations, at its core, corresponds to the monetary resources and pool of skilled talents involved. As Nye observes, "a teenage hacker and a large government can both do considerable damage over the internet, but that does not make them equally powerful."[27]

Hence, advanced cyber operations require significant manpower and financial investment as attackers must comprehend the sophisticated topology of networks. The U.S. and Israel-led Stuxnet virus attack on the Iranian nuclear enrichment facility needed approximately $300 million of investment and took several years of meticulous preparation. Specifically, programmers had to obtain confidential details about "frequency converter drives [and] technical parameters of centrifuges" as well as expensive machinery used to simulate the virus before its deployment.[28] As a result of the labor-intensive and technologically complex process, Stuxnet was able to feature the "first-ever rootkit for a programmable logic controller" and destroyed one-fifth of Iran's nuclear centrifuges.[29] Similarly, the 2015 Russian hacking of the Ukranian power grid required highly demanding logistical procedures including the disruption of power supplies and delivering of "telephone denial of service attack" against customer centers that respond to electricity outages.[30] These examples signal how only a handful of governments have the monetary, technical and intelligence capability to complete large-scale attacks and reinforce the exclusive leadership that great powers possess in cyberspace.

### *2. Defense Network Systems*

In addition to unmatched cyber offense, the strongest nations have the highest quality of defense against intricate malware and can share such a safeguard system to improve collective deterrence by denial. Governments seldom release commentary on cyber defense processes to minimize the possibility of exposing vital information. The lack of transparency, however, does not equate to incompetency. Although the Pentagon alone receives millions of hacking attempts every day, the U.S. government rarely reports cases of noteworthy cyber intrusions. Even the incidents that are regarded as deterrence failures had "relatively modest" effects on national security and never escalated to armed conflicts.[31] The limited impact of cyber attacks, in turn, suggests how the defense system of great powers effectively deterred persistent threats and rendered intrusion attempts futile.

[27] Nye, "Cyber Power," 11.

[28] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1-2 (2014): pp. 4-37.

[29] Ibid.

[30] Craig and Valeriano, "Realism and Cyber Conflict," 5.

[31] Nye, "Deterrence and Dissuasion in Cyberspace," 48-49.

In this sense, through participation in multi-actor organizations, smaller state, and non-state entities can learn about advanced defense structures and utilize obtained knowledge to upgrade their respective systems. Certainly, some may criticize that other actors can devise operations against great powers based on confidential information about their defense technology. These concerns, while valid, can be resolved via strict security-coordination protocols and should not obscure the broader benefits generated by international cooperation. In particular, as major states remain heavily connected to global networks and consist of civil society users, elevating collective defense allows more actors to report "early warning indicators and reveal adversary capabilities."[32] The Biden administration, for instance, set minimum security standards that firms should abide by and further required owners to "report any identified gaps" in internal networks.[33] In turn, the federal government provided a defense advisory on Chinese "state-sponsored cyber techniques" used to exploit the Exchange Server vulnerabilities.[34] All in all, great powers have the competence to empower other stakeholders with stronger network defense and thereby bolster the combined cyber resilience of the coalition.

### *3. Attribution to Advanced Threats*

Dispelling the myth that anonymous challengers can avoid accountability, great powers successfully attribute the "most sophisticated operations with a high level of certainty."[35] Acquiring new information is a costly process: the U.S. allocated $85.8 billion for the intelligence community in 2020.[36] Besides such heavy investment, the Department of Defense has repeatedly stated its strong resolve to "locate and hold potential aggressors accountable for actions that harm America or its interests."[37] Indeed, leaked papers by Edward Snowden in 2014 disclosed how the U.S. National Security Agency (NSA) closely monitored the telecommunications data of millions of citizens and 35 world leaders. Regardless of its moral and legal implications, the incident underlined how, if determined, great powers have sufficient intelligence networks and skilled workforces to surveil against potential sources of risk. Unsurprisingly, the Federal Bureau of Investigation (FBI) arrested Ross Ulbricht, owner of the "biggest anonymous darknet market for illegal drugs," and confiscated around $28.5 million worth of bitcoins.[38] Outside borders, U.S. government agencies pinpointed North Korean state-sponsored actors as the main culprits for cryptocurrency theft in 2021.[39] In essence, relying on their superior law-enforcement and intelligence forces, major states have tracked down malign players who exploit cyberspace under the veil of anonymity.

[32] Brandon Valeriano and Benjamin Jensen, "The Myth of the Cyber Offense: The Case for Restraint," *CATO Institute*, 2019, 9.

[33] "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," The White House (The White House, July 19, 2021).

[34] Ibid.

[35] Rid and Buchanan, Attributing Cyber Attacks, 31.

[36] Office of the Director of National Intelligence, "U.S. intelligence community budget."

[37] Rid and Buchanan, Attributing Cyber Attacks, 27.

[38] Andy Greenberg, "FBI Says It's Seized $28.5 Million in Bitcoins from Ross Ulbricht, Alleged Owner of Silk Road," Forbes, April 16, 2015.

[39] American officials revealed how hackers attempted to steal digital currency from over 30 nations by targeting individuals and companies with malware-corrupted applications (26).

Rather than withholding attributive evidence to themselves, great powers often benefit from disseminating intelligence information and consequently enrich other members of the coalition. Although publicizing intelligence can have undermining implications on national security, “partial revelation of capabilities” bolsters the credibility of the attribution.[40] Upon recognizing Chinese hackers as the culprits of the Microsoft Exchange Server attack in March 2021, the White House shared relevant details with "an unprecedented group of allies and partners" and notified Microsoft on additional liabilities on the system.[41] By releasing evidence for select events, the U.S. could first exhibit its awareness of China's malign cyber activities and establish its trustworthiness for future cases where information-sharing may be more burdensome. Meanwhile, even if the U.S. has all the necessary equipment and funding, unilateral approaches could inevitably narrow its view and outlook. By informing more state and non-state actors, the nation could coordinate multilaterally and "generate new evidence and analysis" on previously overlooked areas.[42] Such reciprocal relationships need not be limited to attribution, as will be discussed in subsequent sections. Ultimately, a multi-actor system allows for a win-win solution: while great powers pressure adversaries by making their message more credible and widening attributive scope, other members can better understand the origins of cyber attack through accessing hard-to-get details.

### *4. Conventional Security Methods*

Adding onto their dominance in cyber operations, great powers can disincentivize malicious activities against the multilateral system by clarifying their intentions to utilize military, financial and diplomatic resources for the cybersecurity of allies. As much as cyberspace presents novel threats, its deterrence measures can, and should, include traditional security measures. Certainly, the cyber domain has enabled multiple actors to “maximize profits while risking little."[43] In turn, great powers also have the right to shift the “confrontation into theaters more convenient to them” by employing conventional military threats and economic sanctions as well as inflicting reputational costs against their adversaries.[44] Indeed, cyber offense alone does not match the level of coercion that armed responses have on the target state’s perception: only four percent of documented cyber operations between 2000 and 2016 yielded “even a temporary political concession.”[45] As a result, successful deterrence methods accompany retributive instruments outside cyberspace and, in extreme cases, involve nuclear weapons as a final resort.

Capitalizing on classical deterrent instruments, great powers can “anchor the deterrence ladder” of coalitions and establish the basis for tangible and impactful punishment.[46] While destructive armaments have yet to be deployed due to the absence of armed-level threats, cyber deterrence ultimately remains “part of general deterrence of hostile acts” and has not been restricted to an eye-for-an-eye approach.[47] In fact, presenting military weapons as a viable option, great powers have long tilted the fundamental

[40] Lupovici, "Cyber Warfare and Deterrence," 57.
[41] The White House Briefing Room, “The United States attributes malicious cyber activity to China.”
[42] Rid and Buchanan, Attributing Cyber Attacks, 27.
[43] Lupovici, "Cyber Warfare and Deterrence," 52.
[44] Ibid., 54.
[45] Valeriano and Jensen, “The Myth of the Cyber Offense,” 5.
[46] Nye, “Deterrence and Dissuasion in Cyberspace,” 55.
[47] Ibid.

conditions of deterrence in their favor. As the existence of conventional weapons imposes "unacceptable costs greater than any intended gain," adversaries grow conscious of retaliatory effects and restrain the intensity of their attacks.[48] Extending such logic to multilateralism, powerful member states can utilize their superior bargaining power and prevent aggression against allied actors from increasing beyond its current scale. Similar to the case of other collective security organizations, the conventional leadership of great powers can ensure the safety of other coalition members by significantly lowering the likelihood of armed-level cyber attacks.

### V. Other State and Non-state Actors: Actualizing Deterrence against Gray Zone Threats

The 2020 Cyber Capability Index identifies multiple states outside the P5, including South Korea, Estonia, Singapore, and the Netherlands, as strongholds of cyber power.[49] Non-state units such as multinational IT companies also have hard-to-penetrate security systems that protect intellectual property and data privacy. As is the case for major states, these entities continually invest in network infrastructure and skilled human capital. Nonetheless, if other state and non-state actors only pursue hard power options, they would be dominated by great powers with unrivaled cyber capacity and lose influence in multilateral settings. Thus underdogs must differentiate themselves in the domain to stay relevant in multi-actor security coalitions.

Consistent with deterrence in other territorial domains, major states can, in principle, mobilize their abundant hard power tools to shut down hostile cyber behaviors. However, as mentioned above, cyber attacks are inferior to conventional military threats in their operational scope and overall impact to national security. Empirically, 257 (i.e. 94 percent) out of 272 cyber incidents had severity scores of less than or equal to 'four'[50] on a scale of one to ten.[51] Given that national resources are finite, countering through destructive cyber or kinetic weapons appears to be excessive in most cases. Governments also lack moral justification as aggressive retaliations overcompensate for the damage suffered by low-tier attacks and escalate tensions further than initial intentions. Accordingly, great powers reserve their most advanced capabilities for existential circumstances and the very instruments that assure the credibility of deterrent threats paradoxically have limited use against the majority of challenges.

In formulating cost-effective deterrence against gray zone attacks, great powers can participate in multi-actor coalitions to draw upon the strong points of other state and non-state participants. Due to their unique position in the international system, smaller state and non-state entities have different advantages within the cyber domain. First, although smaller nations do not lead in absolute amounts, they have clearer stakes to bolster certain areas of cybersecurity and surpass great powers in their 'proportional focus' towards select issues. Second, being the main target of asymmetric threats, corporations and individuals form the basis of societal-level defense against everyday intrusions. Based on their non-governmental status, these actors counter malign activities in more direct and transparent ways than nation-states. Finally,

[48] Jessica Cox,, "Nuclear Deterrence Today," NATO Review, June 8, 2020.
[49] Other notable countries include the Netherlands, Sweden, New Zealand, Israel and Switzerland (Belfer Center, 2020).
[50] Severity of seven or above signals "national-level sustained damage and death" (Valeriano & Jensen, 2019).
[51] Valeriano and Jensen, "The Myth of the Cyber Offense," 11.

owing to their multiplicity, individual users have collective bargaining power and impose moral and economic costs on major state adversaries through their roles as norm entrepreneurs and consumers in the digital economy.

*1. Custom-made and Case-specific Security Models by Smaller states*

Nations with relatively weak military counterbalance deficiencies in hard power resources through specialization. Considering differences in security infrastructure, great powers and other states have diverging perceptions on what constitutes low-level threats: attacks have disproportionate consequences on nations respective to their size and capacity. That being said, unlike major states that try to solidify their hegemony across multiple cyber fields, weaker nations prioritize safeguarding national security and minimizing the associated costs of potential intrusions. Additionally, since these actors lack global influence, their most relevant and credible threats arise from a limited number of adversaries. In this context, smaller powers identify their competitive edge against key intruders and subsequently design cybersecurity postures that accommodate their distinctive strengths.

Indeed, states devise tailored strategies to deepen their expertise on specific security problems caused by a particular set of enemies. As a leading example, Estonia suffered from Russian denial-of-service attacks in 2007 that disabled government, bank, media, and internet service websites. Acknowledging their offensive inferiority, Estonia prioritized cultivating well-trained cyber-defense forces. Ever since, the smallest Baltic nation has implemented “intrusion detection and protection systems" and, most importantly, launched the “world’s largest and most complex real-time network defense exercise” known as Locked Shields.[52] Analogously, the South Korean public and private sector received 1.5 million cyberattacks per day in 2020, mostly from North Korea aimed at stealing money. In response, the government capitalized on the nation’s power in the IT industry to increase responsiveness against hacking attempts. Case in point, the Ministry of ICT shifted away from its reliance on individual reports for detecting malware and started working with data center firms to “collect real-time threat information [available on] social networking services and the dark web.”[53] As a result of these concentrated efforts, Estonia ranks above Russia in the cyber defense index while South Korea outperforms most states in the informational control and commercial sector.[54]

Together, case-specific deterrence methods prepare members of multilateral networks against various risks. Certainly, great powers can to deliver custom responses against low-level attacks and would invest at a larger scale in the necessary technology. Given that each incident has different relevance, however, it is cost-ineffective to become a security expert against all types of aggressions. Moreover, even the most advanced nations are not aware of the “full set of actions and reactions” arising from cyber conflict due to the large volume of actors as well as “problems of unintended consequences.”[55] Taking advantage of the positive-sum traits of cooperation, coalitions can combine individual state strategies into a

[52] e-Estonia, “How Estonia Became a Global Heavyweight in Cyber Security,” e-Estonia, June 14, 2017.
[53] Yoon Hwan Chae, “S. Korea to spend 670 bln won on cybersecurity by 2023,” Yonhap News Agency. February 18, 2021.
[54] Julia Voo et al., National Cyber Power Index 2020, 43.
[55] Nye, “Cyber Power,” 26.

collective knowledge bank and allow states to upgrade deterrence practices by learning from each other's specialized approaches. As direct reactions to real-world challenges, the tried-and-tested methods of smaller powers have empirical value and can be applied to the frontlines of societal-level cyber conflicts. More importantly, although each state individually covers a narrow scope, the combined body can address, in-depth, a wide range of low degree attacks. For example, major states in NATO currently raise public awareness and train skilled personnel by partaking in scenario-based network maintenance simulations developed by Estonia. In the meantime, states can acquire insights into public-private security partnerships from industry-driven nations like Israel and South Korea. Suffice to say, states other than great powers supply distinct deterrence perspectives against gray zone threats.

*2. Defending Civil Society on Asymmetric Vulnerabilities*

Considering their heavy dependence on computer networks, the most connected nations paradoxically have greater attack surfaces—ranging from personal devices to public infrastructure— for adversaries to penetrate. More than two-thirds of the population have access to online devices in developed nations; South Korea, Japan, United Kingdom (U.K.), and Scandinavian countries are the leading states with over 90 percent of the population being Internet users.[56] In contrast, isolationist states, namely North Korea, restrict public access to worldwide networks to control and censor the flow of information.[57] Actors with lower interdependence to the global system could therefore exploit the "digital connectivity of target nations for covert operations" and secure an advantageous position.[58] In short, traditional state-based power holders have more vulnerabilities within cyberspace compared to other territorial spheres grounded in military might.

As constituents of the attack surface, companies and individual experts are well-positioned to hinder exploitative tactics by intruders. The statement that 'cyber attacks are cost-effective tools' depends on the assumption that victims in civil society lack sufficient experience and technological brainpower. Yet, given that their products and consumers are the main targets of frequent hacking attempts, firms deal with cyber incidents daily and utilize their accumulated know-how to update defense practices for future threats. Installed features such as spear-phishing email detection and advanced firewalls automatically filter common types of intrusions against personal devices. Moreover, to preempt potential damage, organizations authorize ethical hackers to break into their machinery, disclose weaknesses, and optimize the system based on the simulation results.[59] These good-willed programmers further serve as educators that transfer their specialized knowledge to a broader audience and, in doing so, equip more people with individual combat ability against basic malware threats. In brief, asymmetric threats can be addressed more directly as the defender and perpetrator reside on the same operational level.

In this context, non-state entities can bridge security gaps in multi-actor systems by publicizing information regarding cyber incidents and providing accessible patches. The private sector operates the majority of infrastructure and forms the basis of communal defense. Unlike intelligence agencies that

[56] Our World in Data, "Internet."
[57] Ibid.
[58] Valeriano and Jense, "The Myth of the Cyber Offense," 4.
[59] EC-Council, "What Is Ethical Hacking?", EC-Council, 2021.

function stealthily in national isolation, corporations are driven by market demands and hence engage in open competition over providing more attributive evidence to appeal to consumers. As a matter of fact, companies make public the most useful and dense reports on attribution.[60] The 2014 Department of Justice document on computer fraud activities by the Chinese People's Liberation Army (PLA) was "less detailed" than that of cybersecurity firms.[61] Adding onto such transparency, experts in security companies have the independent capability to track down malicious schemes and offer user-specific guidance to citizens under threat. Notably, a researcher of CrowdStrike—a cybersecurity technology company based in Silicon Valley—uncovered the PLA's complicity in infiltrating "US defense and European satellite industries" through examination of registration data, internet blogs, photographs on the perpetrator's Picasa page, and positional information.[62] Analysts at major firms including Microsoft, Cisco, and McAfee likewise delivered elaborate breakdowns of the 2017 WannaCrypt malware, uploading pertinent patches for protection. To summarize, by inviting non-state actors into the coalition, governments delegate the work of maintaining cyber hygiene to companies and individuals that can counter threats surrounding civil society in more open and personalized ways.

### *iii) Norms and Associated Economic Costs*

Individuals in cyberspace can contribute to multi-actor deterrence by developing normative taboos at the grassroots. Although official diplomacy and partnerships do not occur at personal levels, states and companies are made up of individuals and their stance reflects the collective beliefs of each constituent. The nuclear taboo stems from a worldwide abhorrence against the destructive and inhumane nature of atomic bombs. While governments practice the inhibition against the first use of nuclear weapons, the consensus among civil society members legitimizes and empowers such normative restraints. In the same vein, as victims of malware attacks on public infrastructure and personal devices, individuals can define specific types of cyber activities as unacceptable and compel their respective states to enact the norm. These processes can also involve communication across borders and pinpoint universal values that worldwide internet users prioritize. Over time, moral restrictions on malicious actions can be internalized as "natural" expectations, codified by professionals into law documents as in the Tallinn Manual, and adopted by multilateral networks as a core founding principle for stabilizing the disordered cyberspace.

Furthermore, developed norms can have actual effects on cyberspace, because of the growing purchasing power of individuals in the digital economy. The surge of multimillionaire social media and search engine platforms serves as testimony to the profitability of online services. In 2006, MySpace had less than 55 million accounts registered; as of 2018, Facebook and Youtube together comprised 4.28 billion users.[63] These firms increase revenue through advertisement based on their ability to attract and retain a user base across the world. Under such a profit structure, individual actors have leverage as their preferences have a decisive influence over the companies' financial gain. In other words, power has shifted from service operators to recipients, as consumers can compare between a wide range of firms before

[60] Rid and Buchanan, Attributing Cyber Attacks, 28.
[61] Ibid.
[62] Nathaniel Hartley, "Hat-Tribution to PLA Unit 61486," Crowdstrike, June 9, 2014.
[63] Our World in Data, "Internet."

making a decision. For this reason, trust-building and brand reputation gain similar prominence to advanced computing technology. While transnational companies initially draw customers through innovative products, they maintain customer loyalty by reinforcing their globally certified status as credible and safe platforms. On the whole, cyber power not only stems from hard power tools but also intangible soft power traits that induce the public to act in certain ways.

Given that consumers have bargaining power, their presence makes attacks counterproductive by imposing reputational costs. For instance, insider reports revealed that Facebook handed over 50 million users' information without consent to Cambridge Analytics consulting firm starting 2015. As a result of violating user privacy agreements, Facebook lost its prestige as a credible international company with individuals boycotting the platform through "#Delete Facebook and #OwnYourData" movements.[64] Statistically, more than 25% of Facebook users deleted the app, including nearly 40% of people aged 18 to 29.[65] The stark decline in user growth and mistrust among younger generations led to a considerable economic downfall: the company lost $120 billion in value and faced legal restrictions following the scandal.[66] Such an event proves that repressive devices backfire in cyberspace where individuals have casting power and, in turn, trustworthy practices that adhere to rule-of-law generate enduring profits. With the economic cost heightened and benefits reduced, norm-sensitive powers restrain themselves from using coercive measures and comply with widely accepted moral standards.

Cumulatively, individuals can enable multilateral coalitions to optimize deterrence by entanglement against major-state adversaries that engage in unethical cyber practices. Over the past decade, China has challenged the American-led liberal international order and devised its own global frameworks including the Belt and Road Initiative. In the cyber realm, China blocked foreign internet web pages through the Great Firewall and developed WeChat as an alternative social media application. However, despite the billion user-base and substantial investment in marketing, WeChat falls behind its U.S. counterparts in global influence. Besides the PRC's authoritarian identity, controversies over espionage and censorship undermine the platform's receptivity among consumers outside of China. According to Dutch researchers, a Chinese database "stored more than 3.7 billion messages," each assigned to a GPS location and country identification number: 19 million of the surveilled communication had been sent from abroad.[67] Reflective of their prejudice toward sexual minorities, WeChat also deleted the accounts of LGBT students in domestic universities.[68] As in the case of Facebook, these actions directly challenge the existing norms that value privacy and freedom and hence undercut the potential revenue streams of the platform. Provided that China has a high degree of interdependence with the global market, the nation may refrain from intrusive operations, gradually change its stance toward joining multilateral frameworks and, in doing so, restore its national reputation among foreign consumers. In short,

[64] Andrew Perrin, "Americans Are Changing Their Relationship with Facebook," Pew Research Center, September 5, 2018.

[65] Ibid.

[66] Shweta Ganjoo, "Facebook loses over 120 billion in market cap," India Today, July 26, 2018.

[67] Emily Feng, "China Intercepts WeChat Texts from U.S. And Abroad," NPR. August 29, 2019.

[68] Yong Xiong, "China Widens Crackdown on LGBTQ Groups and Content," CNN, July 7, 2021.

individuals in like-minded states can burden and dissuade great powers pursuing cyber attacks through their roles as norm-conscious consumers.

## 6) Conclusion

The study delved into the successful conditions and inner-working mechanisms for multi-actor deterrence and outlined the contributions of each stakeholder. Multilateral coalitions provide distinct incentives for membership as well as the cost of opting-out; this shifts the decision matrix of actors toward joining the institution and ensures the regime's sustainability. Smaller states and non-state actors have the benefit of strengthening their cyber defense, offense, and attributive credibility through coordinating with great powers. Extended deterrence through traditional security measures further limits the possibility of armed-level attacks in cyberspace. Conversely, states with weaker military capabilities share their custom-made strategies against a specific set of adversaries and enable coalition members to prepare against gray zone threats at an efficient price. Likewise, non-state actors such as private corporations and expert programmers actualize deterrence by applying defense and attribution methods to protect civil society from impending intrusions. Finally, given the importance of reputation and credibility in the internet era, users around the world initiate discussions on normative regulations and help states maximize the cost of entanglement through collective moral and economic pressure.

Adding onto the security incentives discussed throughout the paper, future studies can analyze how multilateral networks provide participants with clear political and monetary benefits. The importance of soft power in cyberspace provides unique opportunities to great powers seeking leadership through norms. Moreover, through multilateral alliances, smaller states can benefit from confidence-building measures and obtain leverage in transactions through their expertise in certain security fields. The safeguarded multilateral system also guarantees stability to individuals and companies heavily dependent on cyberspace for daily activities. Specifically, the firms can bolster marketability through enrolling in international trust certifications and further reduce perceived risks in foreign investments by branching out to countries that partake in the coalition.

To conclude, cybersecurity coalitions comprising state and non-state actors allow for the complementation and, by extension, optimization of different dissuasion measures. In proving this assertion, the paper also refuted two misleading arguments in cyberspace regarding power diffusion and the adaption of nuclear deterrence. Contrary to the claims that weak actors will replace the most powerful nations, great powers remain the strongest forces in cyberspace. Yet, the overemphasis on large-scale hard power creates asymmetries that opponents can exploit and hence smaller state and non-state entities have opportunities to capitalize on their positional advantage. After all, rather than being mutually exclusive, the findings reinforce each other to necessitate the role of multilateralism in deriving positive-sum solutions for cybersecurity.

## Bibliography

### *Articles and Books*

Craig, Anthony, and Brandon Valeriano. "Realism and Cyber Conflict: Security in the Digital Age." *E-International Relations*, 2018, 1–11.

Lawson, Sean. "Putting the 'WAR' IN Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United State." *First Monday* 17, no. 7 (2012). https://doi.org/10.5210/fm.v17i7.3848.

Lee, Seungjoo. "The International Political Economy of Digital Trade Order: The Divergence of Digital Trade Strategies and the Complexity of Cleavage Structures" (In Korean). *Journal of Northeast Area Studies* 25, no. 2 (2020): 53-80.

Lupovici, Amir. "Cyber Warfare and Deterrence; Trends and Challenges in Research." *Military and Strategic Affairs* 3, no. 3 (2011): 49–62.

Medeiros, Breno Pauli, and Luiz Rogeiro Franco Goldoni. "The Fundamental Conceptual Trinity of Cyberspace." *Contexto International* 42, no. 1 (2020): 31–48.

Nye, Joseph. *Cyber Power*. Cambridge, MA: Harvard Kennedy School Belfer Center for Science and International Affairs, 2010.

— "Nuclear Lessons for Cybersecurity?" *Strategic Studies Quarterly* 5, no. 4 (2011): 18–38. https://doi.org/10.21236/ada553620.

— "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (2017): 44–71. https://doi.org/10.1162/isec_a_00266.

Office of Management and Budget. *Budget of the U.S. Government*. Washington: The White House, 2021.

Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1-2 (2014): 4–37. https://doi.org/10.1080/01402390.2014.977382.

Urgessa, Worku Gedefa. "Multilateral cybersecurity governance: Divergent conceptualizations and its origin." *Comput. Law Secur. Rev.* 36 (2020): 105368.

Valeriano, Brandon, and Benjamin Jensen. "The Myth of the Cyber Offense: The Case for Restraint." *CATO Institute*, 2019. https://doi.org/10.1163/2210-7975_hrd-9985-20190056.

Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Daniel Cassidy, and Anina Schwarzenbach. *National Cyber Power Index 2020*. Cambridge, MA: Harvard Kennedy School Belfer Center for Science and International Affairs, 2020.

### *Media Reports and Primary Sources*

Chae, Yoonhwan. "S. Korea to spend 670 bln won on cybersecurity by 2023." Yonhap News Agency. February 18, 2021. https://en.yna.co.kr/view/AEN20210218006100320.

Cox, Jessica. "Nuclear Deterrence Today." NATO Review. June 8, 2020. https://www.nato.int/docu/review/articles/2020/06/08/nuclear-deterrence-today/index.html.

Coy, Peter. "U.S. Policy on China May Move from 'America First' to America & Co." Bloomberg. December 9, 2020.

https://www.bloomberg.com/news/articles/2020-12-09/u-s-policy-against-china-america-first-is-becoming-america-and-others?sref=RfJLbe1B.

EC-Council. “What Is Ethical Hacking?” EC-Council. 2021. https://www.eccouncil.org/ethical-hacking/.

e-Estonia. “How Estonia Became a Global Heavyweight in Cyber Security.” e-Estonia. June 14, 2017. https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/.

Feng, Emily. “China Intercepts WeChat Texts from U.S. And Abroad, Researchers Say.” NPR. August 29, 2019. https://www.npr.org/2019/08/29/751116338/china-intercepts-wechat-texts-from-u-s-and-abroad-researcher-says.

Ganjoo, Shweta. “Facebook loses over 120 billion in market cap.” India Today. July 26, 2018. https://www.indiatoday.in/technology/news/story/facebook-loses-over-120-billion-in-market-cap-after-privacy-scandal-hits-revenue-user-growth-1296533-2018-07-26.

Greenberg, Andy. “FBI Says It’s Seized $28.5 Million in Bitcoins from Ross Ulbricht, Alleged Owner of Silk Road.” Forbes. April 16, 2015. https://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/?sh=72e095af2765.

Hartley, Nathaniel. “Hat-Tribution to PLA Unit 61486.” Crowdstrike. June 9, 2014. https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/.

Perlroth, Nicole. “In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back .” The New York Times. October 23, 2012. https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

Perrin, Andrew. “Americans Are Changing Their Relationship with Facebook.” Pew Research Center. September 5, 2018. https://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/.

Roser, Max, Hannah Ritchie, and Esteban Ortiz-Ospina. “Internet.” Our World in Data. July 14, 2015. https://ourworldindata.org/internet.

The United States Department of State. “The Clean Network.” The United States Department of State. January 17, 2021. https://2017-2021.state.gov/the-clean-network/index.html.

The White House Briefing Room. “The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People’s Republic of China.” The White House. July 19, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/

Xiong, Yong. “China Widens Crackdown on LGBTQ Groups and Content.” CNN. July 7, 2021. https://edition.cnn.com/2021/07/07/business/china-lgbt-wechat-censorship-intl-hnk/index.html.