Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Sanjay Goel, *Connections QJ* 19, no. 1 (2020): 73-86
https://doi.org/10.11610/Connections.19.1.07

Research Article

National Cyber Security Strategy and the Emergence of Strong Digital Borders

Sanjay Goel

New York State Center for Information Forensics and Assurance, University at Albany, 1400 Washington Avenue, Albany, NY 12222

https://www.albany.edu/cifa/

Abstract: The growth of the Internet and innovation that thrived with it was facilitated by an environment relatively free of controls. Regrettably, however, with its deep integration into the societal framework, the Internet has become a potent tool for influencing geopolitical conflicts, including interference in internal affairs of other nations, undermining national security, destabilizing financial infrastructure, and attacks on critical infrastructure. While countries are harvesting the social and economic benefits of the Internet, they are frightened of the threats it poses to national security. In response to these threats, countries are starting to tighten their internet borders and developing their cyber weaponry both as a deterrent to, and leverage during conflicts. A potential downside of such state-by-state regulation is inhibition of the rapid innovation that the Internet has traditionally fostered and the curtailing of freedom of speech that has led to the social integration in the society. On the other hand, innovation and freedom cannot thrive in a chaotic environment with rampant crime and a lack of rules, norms, and ethics. With this in mind, national policymakers face the challenge of striking a balance between regulation and potential chaos on the Internet while at the same time promoting freedom. In efforts to strike such a balance of national interests, borders in cyberspace have an important role to play along with international efforts to build trust in cyberspace and to slow down the fragmentation of the Internet. This article discusses how cyber conflicts are escalating, how mutual distrust is growing, and how nation-states are adapting to the constantly changing cyber domain.

Keywords: Cyber threats, critical infrastructure, cyber conflict, international law.

Introduction

Sophistication and impact have continuously escalated since the first Morris worm cyberattack in 1988 [1] and have recently become a key part of national defense strategies of several countries. Cyber is now considered a separate domain of conflict along with land, sea, air, and space, clearly indicated in military doctrines of the strongest nations in the world, i.e., Russia, China, and the US. Each country is shoring up their defenses and, at the same time, working furiously to develop cyber weapons and probe the cyber defenses of other countries. Cyberattacks have already been used to complement military interventions, retaliate against the policies and actions of other countries, and to interfere in the elections of other countries. A fierce cyber arms race has ensued with no signs of abatement. Nation states now face a dilemma on whether to work cooperatively to de-escalate the cyber arms race and allow the Internet to prosper unfettered, or to put borders on the Internet and threaten its growth and evolution.

There have been several attempts at treaty formation for containing the growth of cyber weaponry; however, lack of attribution, increasing vulnerabilities, escalation in economic rivalries among nations are making consensus building around these treaties hard. While attribution around cyber incidents is getting better based on improved analytic techniques, the development activities of nations around cyber weapons are still sheathed. A game-theoretic view of the situation suggests that each country needs to keep maximizing its cyber arsenal, assuming that other countries are maximizing their efforts at developing cyber arsenals. The earliest cases of cyber warfare occurred in conflicts between Russia and the former Soviet republics of Georgia and Estonia. In those cases, attacks were used for media propaganda, defacement of websites, etc. Over time, however, cyberattacks are becoming more sophisticated, targeted, and dangerous. Also, more nation states are embracing cyberattacks and using the attacks strategically to meet their geopolitical objectives.

This article frames the current challenges and discusses the potential outcomes of this conflict. In section 2 it lists key incidents over the last two decades that show the escalation of the sophistication and impact of nation-state cyberattacks. Section 3 discusses how the future evolution of the Internet exponentially increases the threat landscape. Section 4 discusses how countries are reacting to the escalation of cyber threats by tightening Internet borders and launching a regime of monitoring and censorship within their borders. Section 5 discusses international efforts at building trust and cooperation in cyberspace to avoid the balkanization of the Internet and to slow down the cyber arms race.

[1] Craig Timberg, "Net of Insecurity: A Flaw in the Design," *The Washington Post*, May 30, 2015, accessed August 13, 2018, https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1.

The Evolution of Cyber Warfare

Operation Aurora, originating from China in 2006, is a targeted malware attack against at least 30 major companies—including Google and Adobe—which exploited a zero-day flaw in Internet Explorer. The exploit allowed malware to load onto users' computers. Hackers seem to have accessed the source code for numerous software products. Five members of Unit 61398 of the People's Liberation Army were "assigned" to deploy a widespread spear-phishing (or "spearfishing") campaign to allegedly hack into leading US companies. The attack involved breaches at 141 companies spanning 20 major industries from 2006 to 2014. Hackers went after American trade secrets: from Westinghouse, for example, the hackers are alleged to have taken plans for a certain type of nuclear power plant. This was the first time the term "advanced persistent threat" was coined.

Stuxnet, discovered in 2010, was a worm that some researchers suggest was developed by the United States and Israel for targeting the Iranian nuclear program by infecting the programming logic controllers (PLCs) of the centrifuges in Iranian reactors. It is thought that the malware may have been introduced through thumb drives of nuclear inspectors sent to Iran through the IAEA. The malware destroyed the centrifuges by changing their rotational speeds beyond their range of operations.

Operation Cleaver, originating from Iran in 2012, conducted a significant global surveillance and infiltration campaign, including the US Navy. It successfully evaded detection and leveraged common tools to attack and compromise targets around the globe. The targets included military, oil and gas, energy and utilities, transportation, airlines, airports, hospitals, telecommunications, technology, education, aerospace, Defense Industrial Base (DIB), chemical companies, and governments. The attack resulted in the theft of sensitive information or took control of critical infrastructure networks in many countries, including Canada, China, England, France, Germany, India, Israel, Kuwait, Mexico, Pakistan, Qatar, Saudi Arabia, South Korea, Turkey, the United Arab Emirates, and the United States.

OPM Attack. The office of Public Management (OPM) attack started in March 2014, targeting US government data and leading to the theft of over 21 million data records. The hack compromised personal information (social security numbers, dates of birth, addresses, etc.) and detailed security-clearance-related background information. Attackers gained valid user credentials to the systems they were attacking, likely through social engineering. The breach involved installation of a malware package within OPM's network and established a backdoor. From there, attackers escalated their privileges to gain access to other OPM systems and data.

DNC Breach. During the 2016 US elections, an attack was orchestrated from Russia to the email servers for the Democratic National Committee (DNC) and the Gmail account for Clinton campaign chairman John Podesta. At least 60,000 emails were stolen and subsequently published by Wikileaks, leading to the res-

ignations of top officials and a major embarrassment for the DNC and the Clinton Campaign.

NotPetya. In 2017, the malware NotPetya spread from the servers of an unassuming Ukrainian software firm to some of the largest businesses worldwide, paralyzing their operations. Some of the damages of major corporations included Merck, which lost 870 million, FedEx, which lost 400 million, Saint-Gobain, which lost 384 million, and Maersk, which lost 300 million, with a total loss of over 10 billion dollars. It is suspected that the attack was launched at the behest of the Russian military.

Each of these attacks represents a clear political objective, i.e., interfering in elections, causing economic impact during conflict, retaliation against an attack, and gathering military intelligence. The ramifications of the attacks are becoming more and more dangerous, and the adventurism of countries continues to increase. Countries are resorting to cyber attacks instead of conventional attacks due to the nebulous attribution and less fear of international condemnation. The stakes are going to get even higher as cyber-physical systems mature and gain mainstream acceptance in society, i.e., self-driving cars, implantable and wearable devices, and smart metering. These ramifications are discussed in the next section.

The Expanding Vulnerability Landscape

Three major innovations of this decade are the smart grid, connected vehicles, and human implantable devices. All three will radically transform society in many ways, some of which cannot be currently conceived. A lot of the discussion around cyber-physical systems is very timely, as the implications of cyber-physical systems on the future of society are enormous.

We are creating three classes of networks: a monolithic network of devices and sensors on the power grid; millions of ad hoc networks in the traffic grid; and a huge personal network in wearables. There are massive challenges in each of them. Most of the discussion here has been pertinent to the static networks of cyber-physical systems such as industrial control, power, and gas distribution. What we have not addressed are the constantly changing networks of connected vehicles and wearable technologies. Let us take a closer look at IOT evolution.

Gartner has estimated that there will be 21 billion employed IoT devices within the next couple of years. Cisco is estimating 50 billion devices, and Intel is taking it further, with a prediction of 200 billion IoT devices.[2] And truly, we are just beginning to understand the potential and promise of the Internet of Things. The range of possible benefits is expanding as adoption increases, with greater efficiency, streamlined processes, and reduced costs being top benefits realized

[2] Nathan Eddy, "Gartner: 21 Billion IoT Devices to Invade By 2020," *Information Week*, October 11, 2015, accessed April 11, 2018, https://www.informationweek.com/mobile/mobile-devices/gartner-21-billion-iot-devices-to-invade-by-2020/d/d-id/1323081.

by all manner of business enterprises. The first revolution came with the creation of the power loom (1784). The second industrial revolution came with the assembly line (1870), and the third industrial revolution came with PLCs (1969). The fourth revolution is happening now and is being driven by sensors, Artificial Intelligence (AI), and robotics.

Imagine for a moment smart farming and the advances in production and prediction that will be realized when sensors can deliver fine-tuned information about temperatures and humidity, soil pH and nutrient levels, to inform farming practices and increase crop yields. Or the remarkable potential in medicine and biomedical informatics of insulin pumps that can monitor blood sugar levels and adjust insulin levels *in real-time*, or IBM's Medical Sieve, which, driven by smart algorithms and advanced AI, sorts through a patient's complete medical history, looking for clues to inform its analysis of the patient's images; learning everything there is to know about the individual in seconds for a smarter diagnosis and an infinitely more personalized treatment plan.[3]

Imagine recapturing the time you currently spend fighting traffic on your daily commute, for reading or even daydreaming, in your self-driving vehicle. The University at Albany is working on a project where traffic signals can communicate with each other, making adjustments to increase traffic flow. Imagine sensors that can predict earthquakes *before* they happen; and the improvements that could be made with greater real-time energy consumption and environmental performance monitoring. IoT has transformed the world of energy generation and transformation. Today we are building an architecture of the power grid that will integrate multiple disparate power grids and make it more resilient. By overlaying a communication grid on top of the power grid and creating an information network that can connect sensors throughout the grid to make it resilient, an integrated electricity market is created where everyone can buy and sell electricity.

Today, 54% of people worldwide live in cities, a proportion that is expected to reach 66% by 2050. Combined with the overall population growth, urbanization will add another 2.5 billion people to cities over the next three decades. Rapid urbanization is causing severe environmental strain. Environmental, social, and economic sustainability must keep pace with this rapid expansion, which is taxing our cities' resources. The goal of smart cities is to promote sustainable development to manage urbanization challenges. By leveraging data efficiently from infrastructure and urban communities' own needs, cities can improve energy distribution, streamline trash collection, decrease traffic congestion, and even improve air quality with help from the IoT.

---

[3] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in *Proceedings of 2012 10th International Conference on Frontiers of Information Technology (FIT)* (Institute of Electrical and Electronics Engineers, December 2012), 257-260, https://doi.org/10.1109/FIT.2012.53.

How can we defend against hacking, cyber-attacks, and data theft? In cities where multiple participants are sharing information, how do we trust that participants are who they say they are? And how do we know that the data they report is true and accurate? With this unlimited promise comes tremendous risk in terms of security and privacy losses, system breaches, and hacking. When critical infrastructure, such as power stations, water supplies, airports, and hospitals, are governed by IoT systems, the potential for loss of life—from failures and cybercriminal activity—rises exponentially.[4]

The *risks* of IoT are not projections either; they are also here. According to a Hewlett Packard study, 80% of tested IoT devices (they tested commonly used home alarms and thermostats, garage door openers, etc.) raised privacy concerns, with an average of 25 security holes per device.[5] In 2016, a DDoS attack—the largest in history—was launched on a service provider using an IoT bot with malware called Mirai, which led to huge portions of the Internet—including Twitter, Netflix, Reddit—going down. Mirai, once in, causes computers to continually search the Internet for vulnerable IoT devices and, using default usernames and passwords to initiate logins, infects them with Mirai also.

The security of our future—the IoT era—will only be as strong as the security of each of the billions of small connected devices that comprise our systems. We have all experienced a computer crashing and losing a document or a spreadsheet, but imagine a pacemaker or digitalized insulin pump that can be hacked, ending a life, or Volkswagen hacking their own cars to bypass emissions-control limitations. Imagine hackers gaining access to bank data and emptying accounts. Unauthorized personnel could access smart devices that store sensitive financial account information, passwords, and other information, exploiting these vulnerabilities to commit identity theft or fraud. A report published by the US Federal Trade Commission estimated that 10,000 households could generate 150 million data points daily, providing a significant number of entry points for hackers.[6]

Nation states are aware of these vulnerabilities and will seek to improve their leverage on other countries by exercising more sovereignty on the Internet. The concept of digital borders and Internet sovereignty has moved on from concept to actuality and several countries are working on controlling information flow across their borders as well as actively monitor and censor information within their border as we discuss in the next section.

---

[4] Tianlong Yu, Vyas Sekar, Srinivasan Seshan, Yuvraj Agarwal, and Chenren Xu, "Handling a Trillion (Unfixable) Flaws on a Billion Devices: Rethinking Network Security for the Internet-of-Things," in *Proceedings of the 14th ACM Workshop on Hot Topics in Networks* (ACM, November 2015), http://dx.doi.org/10.1145/2834050.2834095.

[5] "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack," *HP News*, July 29, 2014, https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676.

[6] Federal Trade Commission, "Internet of Things: Privacy and Security in a Connected World," FTC Staff Report (January 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

Balkanization of the Internet

The Internet has operated with free access and international sovereignty for many years, allowing it to grow and develop into a ubiquitous communication platform that now also acts as a social glue for society and a platform for commerce and trade. One argument for opposing Internet restrictions is that information is an international human right. The more practical and economically powerful argument is that international trade is contingent on Internet access and cross-border data flows. The free and open access of the Internet is what made it very successful – but that success has also become its biggest challenge.

The Internet's enormous power in influencing public opinion and driving trade has made it a target for militarization. As US Defense Secretary Panetta observed, "the Internet is open. It's highly accessible, as it should be. But that also presents new terrain for warfare. It is a battlefield of the future."[7] It is being used to influence public opinion and support regime change, to launch attacks on nation-states' information infrastructure, to recruit new members for terrorist organizations, and to disrupt and endanger critical infrastructure. What is unique about cyberspace (in relation to other physical domains like land, air, and space) is that it is global, but with a remarkably low cost of entry.

Propaganda and dissent have long been active forces in countries, but the sheer scale and reach of the Internet have made it a powerful weapon. Whether it is videos of protests or police brutality on YouTube, or new broadly effective Internet canvassing tools, the Internet is playing a powerful role in political organizing. Actors—even individual actors—can affect power in cyberspace that are orders of magnitude higher than what can be achieved by the small set of nations that operate with the consequence in the land, air, maritime, and space operational domains.

The Internet is a domain in which all other operational domains and national instruments of power are enabled (if not dependent). Given the tremendous power of the Internet, and in response to its use for political and military purposes, the concept of international Internet sovereignty is rapidly shifting towards the concept of sovereign Internet borders. This transformation is accelerating the pace of tightening Internet borders in recent years. Governments from China to Iran to Burma are increasingly filtering and blocking access to media and blogs that advocate political views that the government disagrees with.

The original and essentially libertarian nature of the Internet is increasingly being challenged by government assertions of jurisdiction over the Internet or the development of rules that restrict the ability of individuals and companies to access the Internet and move data across borders. The tools available for restricting access to the Internet and cross-border data flows are becoming increasingly available, complex, and broadly adaptable. These include blocking the backbone or access points into the country and the filtering of domain names,

[7] Joshua P. Meltzer, "The Internet, Cross-Border Data Flows and International Trade," *SSRN Electronic Journal*, April 1, 2013, http://dx.doi.org/10.2139/ssrn.2292477.

Internet protocols, or URLs. Governments can also indirectly restrict access to the Internet by restrictive regulations that essentially limit search engines, for example by conditioning operating licenses on not posting particular material, and imposing stiff penalties for non-compliance. Control of information—for countries choosing to go that route—includes limiting access to foreign information sources, blocking foreign Internet tools such as Google search, Facebook, Twitter, and selected mobile apps, and requiring foreign companies to adapt to domestic regulations.[8] However, as we put more and more controls in place, we are throttling the Internet and making it slower. The legitimacy of the government in enforcing national borders on the Internet comes from rules legislated ostensibly to protect citizens from deleterious external influence.

Let us look at the increasing Balkanization of the Internet, as some countries work to establish national boundaries while others fight for the Internet's original open-access internationalism. We will then look more closely at this dichotomy in the context of the growing militarization of the Internet and cyber warfare. Is it a false dichotomy, with even those countries—like the United States—advocating for a borderless Internet involved in cyber warfare and defense? Let us first examine the landscape of Internet borders – who is doing what?

Tightening Internet Borders for National Security

The emergence of the Internet in China has transformed the Chinese media from a closed and centralized system to an open and decentralized system. China has also seen a new population actively engaged on the Internet.[9] By the end of 2017, China had 772 million Internet users, with a penetration rate of 55.8%, and had become the largest online population in the world. China has significantly expanded the technological capacity and human capital devoted to controlling Internet content, including employing an estimated 500,000-2 million Internet propagandists (more popularly known as 50cent army), to write the Internet comments to safeguard the prestige and integrity of the Chinese Communist Party.[10]

China, Saudi Arabia, Iran, and others have similar aspirations for the Internet: they think governments should get to decide what information flows across their borders, not companies and NGOs. A Freedom House 2018 report examined 65

[8] Meltzer, "The Internet, Cross-Border Data Flows."

[9] Wenfang Tang and Shanto Iyengar, eds., *Political Communication in China: Convergence or Divergence Between the Media and Political System?* (London: Routledge, 2012).

[10] Tenzin Dalha, "Assertion of China's Sovereignty over the Internet," *global-is-asian*, October 4, 2018, https://lkyspp.nus.edu.sg/gia/article/assertion-of-china's-sovereignty-over-the-internet.

countries and found that since the previous year Internet freedom declined in 26 of them, with almost half of those declines related to elections.[11]

China, as the architect of "cyber-sovereignty" has begun exporting its Internet censorship regime to other countries, changing the Internet from the bottom up. According to the Freedom House report, at least 36 governments (including Jordan, Egypt, Saudi Arabia, and Vietnam) have received closed-door Chinese training on "new media and information management." For the past couple of years, China has hosted media officials from dozens of countries for two and three-week seminars on its censorship and surveillance system and supplied telecommunications hardware, advanced facial-recognition technology, and data-analytics tools to a variety of governments with poor human rights records. There is evidence that some countries, like Uganda, are using Chinese-made software to monitor their local Internets, ostensibly to fight crime.

Given broad-range global cyber incidents like NotPetya, interference in elections, and the insecurity that these incidents can sow, many countries are taking a more authoritarian approach to the Internet. A November 2018 cybercrime resolution backed by Russia and adopted by the UN General Assembly, saw three of the biggest democracies in the world—India, Brazil, and Nigeria—voting with Russia and China, clashing with more traditionally open countries including Australia, Canada, Estonia, France, Greece, Israel, the United States, and the United Kingdom. Late 2018 and early 2019 also saw the adoption of laws being passed or proposed that limit Internet freedoms in the name of mitigating vulnerability and combating cybercrime in Vietnam, Thailand, Egypt, the United Arab Emirates, and Tanzania.[12]

Russia's government is tightening its control over the Internet, and Russia is not alone. In the lead-up to the 2018 election of Putin to his second term, authorities increased their already tight grip on the Internet blocking Telegram, the popular messaging service with over 10 million Russian users, because the platform refused to provide encryption keys to the FSB. There were protests against the legislative push to isolate Russia's Internet by making it self-sufficient, supposedly to guard against external "threats." Critics warn that the so-called "sovereign" Internet law will act as a sort of digital "iron curtain," and serve as a tool for the government to impose censorship on dissenting views on social media. Reports suggest that Chinese and Russian-style paranoia about unrestricted online discourse is beginning to resonate in the West. Kieron O'Hara, a computer science professor and expert on Internet governance, says Western democracies

[11] Adrian Shahbaz, "Freedom on the Net 2018: The Rise of Digital Authoritarianism," Freedom House, 2018, https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

[12] Justin Sherman, "How to Regulate the Internet Without Becoming a Dictator," Foreign Policy, February 18, 2019, https://foreignpolicy.com/2019/02/18/how-to-regulate-the-internet-without-becoming-a-dictator-uk-britain-cybersecurity-china-russia-data-content-filtering.

are converging with China and Russia on common fears, leading to a shared affinity for something like an "authoritarian Internet" model.[13]

This tightening is not only an Eastern phenomenon—after interference in US presidential elections, there has been considerable debate on how to control propaganda on social media—which is a form of censorship. Internet media companies like Facebook and Google are being asked to take the lead in rooting out fake news from their websites. Some might see a big difference, though when one considers that the United States is attempting to root out false information, where some of the other countries are trying to root out genuine debate among its own citizens.

The economy and societies around the world are intricately woven with the Internet across the entire spectrum of society, including commerce, communication, education, and social relationships. The escalation of cyberattacks, interference in internal politics, and the potential for loss of lives and property should give nations pause. There have been several efforts to contain the cyber warfare arena through efforts to build cyber treaties and norms, as discussed below.

Diplomatic Brakes to De-escalate Cyber Arms Race

There is much debate on the norms and code of conduct in cyberspace. Ideally, the norms should focus on keeping a free flow of information on the Internet to empower people. However, the discussion has shifted to who, what and when there can be an attack on the Internet and the consequences of these attacks.

Three GGEs (Groups of Governmental Experts on Information Security) in the UN before 2016/2017 had established and carried forward an international conversation on cybersecurity since 2010, mainly on norms and confidence-building measures in cyberspace. The 2016/2017 group was tasked with determining "how international law applies to the use of information and communications technologies by states." This issue—international law and its application—is a critical sticking point.

Authored by nineteen international law experts, the "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" was published in 2017, updating the 2013 analysis on how existing international law applies to cyberspace. It is notable that the new edition, just four years after, included a change in the book's title referring to "cyber warfare" to "cyber operations;" a reflection that in today's world cyberattacks usually fall well below the threshold at which international law would typically declare them to be a formal act of war.[14]

The OSCE has also been working on developing confidence-building measures (CBMs) for the last several years and has had some success in building consensus on preliminary points. The primary goal of these CBMs is to enhance transpar-

[13] Eduard Saakashvili, "The Global Rise of Internet Sovereignty," *.coda*, March 21, 2019, https://codastory.com/authoritarian-tech/global-rise-internet-sovereignty/.

[14] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

ency between states by promoting exchanges of information and communication between policy and decision-makers. The hope is that while these CBMs will not stop an intentional conflict, they can possibly mitigate an unintentional action by slowing down the escalation of events.

US's operational norms in air, land, and maritime domains are derived fundamentally from the concept of Westphalian sovereignty: "all members shall refrain in their international relations from the use of force against the territorial integrity or political independence of any state,"[15] or responsible behavior should default to a pattern of operational restraint.

Without agreement on international law and its application to the cyber domain, including verification and attribution of incidents, many other aspects (including norms, confidence-building measures, and capacity-building) remain up in the air, as viewpoints seem to be diverging and solidifying rather than converging. One core question of the cyber domain is whether cyber operations—which most if not all countries engage in—follow a pattern of operational restraint or escalation.

Are Cyber Attacks Retaliatory or Strategic Actions by the Nation States

Are cyber operations primarily restrained? Are they meant to be escalatory or not? Are they effective as foreign policy instruments and maneuvers? Some would counter that the characteristics of cyberspace—including the uncertainty of effects and response, and the central lack of attribution and verification—seem, by their very nature, to be escalatory. But are they? One thrust to inform international policy is to understand better and quantify our present reality. A recent policy analysis paper from the Cato Institute looked at 272 documented cyber exchanges between rival states between 2000 and 2016. In categorizing those exchanges, they estimated 32% as disruptions, 54% as espionage, and 12% as degradation, or the most damaging types of attacks, meant to disable or fundamentally damage their targets. Most importantly, the study's authors concluded that most (68%) do not document a pattern of retaliation, concluding that most cyber operations do not beget attacks, nor do they deter them. They posit that a certain level of cyber operations is the norm and that while cyberspace to date has been a domain of political warfare and coercive diplomacy, cyber operations have not been escalatory or particularly effective in achieving decisive outcomes.[16] "Incidents" or "attacks," regardless of their number, do not constitute a war—cyber or otherwise—in a true political, legal, operative, or factual sense.[17] While many talk of a coming "Cyber Pearl Harbor," the authors sug-

[15] Charter of the United Nations, effective 24 October 1945, Article 2(4).

[16] Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford Scholarship Online, May 2018), https://doi.org/10.1093/oso/9780190618094.001.0001.

[17] Mika Kerttunen and Eneken Tikk, "Strategically Normative. Norms and Principles in National Cybersecurity Strategies," *EU Cyber Direct*, April 13, 2019,

gest the domain is really littered with covert operations meant to manage escalation and deter future attacks. They counsel a defensive posture consisting of limited cyber operations aimed at restraining rivals and avoiding escalation instead of recent policy changes and strategy pronouncements by the Trump administration that suggests that offense is an effective and easy way to stop rival states from hacking America (a posture the authors note as a dangerous myth).

Some argue that cyber operations offer an effective means to diffuse and de-escalate, and rather than persistent action and preemptive strikes, America needs to use cyber operations to sow persistent deception and active defenses.

International Politics as a Tool for Managing Cyber Relations

A central component of President Obama's position was cyber deterrence and working towards international norms of behavior. His 2011 International Strategy for Cyberspace laid out three core principles: 1) ensuring fundamental freedoms such as freedom of expression; 2) privacy; and 3) the free flow of information. In 2015 Obama reached a deal with the Chinese to limit cyberattacks, with a subsequent reduction in their number. President Trump has taken a different position, sparking increased Sino-American tensions with trade policies and a US Cyber Command position [18] calling for "persistent action to maintain cyber superiority." His position is one of active engagement and defending against outside networks. Do such aggressive stances and policies for authorizing preemptive offensive cyber strategies risk crossing a threshold and changing the rules of the game?

In May 2019, the NATO Secretary General told Russia and other potential foes that the Western military alliance was ready to use any and all possible means at its disposal to respond to cyberattacks. "For deterrence to have full effect, potential attackers must know we are not limited to respond in cyber space when we are attacked in cyber space," Stoltenberg said during a joint press appearance in London with UK Foreign Secretary Jeremy Hunt. "We can and will use the full range of capabilities at our disposal." [19] Do such aggressive stances and policies for authorizing preemptive offensive cyber strategies risk crossing a threshold and changing the rules of the game?

---

https://eucyberdirect.eu/content_research/a-normative-analysis-of-national-cybersecurity-strategies/.

[18] United States Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," June 14, 2018, www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

[19] "NATO Warns Russia of 'Full Range' of Responses to Cyberattack," *Security Week*, May 23, 2019, https://www.securityweek.com/nato-warns-russia-full-range-responses-cyberattack.

Conclusions

A number of nation state-linked cyber threats have emerged over the last decade that have left nations feeling insecure, including surveillance/attacks on critical infrastructure, interference in internal affairs of other countries through Internet/social media-based propaganda, financial fraud, theft of intellectual property, and compromising national security. In reacting to these threats, nations are tightening their Internet borders. Unless countries feel secure, this tightening of Internet borders will continue and spread rapidly, and until the Internet is truly demilitarized, countries will not feel secure. In the absence of effective and verifiable norms, we should expect to see a continued tightening of Internet borders and increased surveillance of the Internet and social media. Countries will continue to build their cyber arsenals as a deterrent against other nations; this will include misinformation campaigns, destabilizing attacks, probing cyber defenses, and gathering intelligence. Without trust and mutual cooperation, it will be hard to build consensus on norms, and this trend will continue and could lead to the eventual complete fragmentation of the Internet; perhaps in a classic East-West divide, which is not a desirable state.

First, if we let this trend continue unmitigated, we will be retreating from much of the gains we have already realized and limit the opportunity to continue to reap rich rewards from our connectivity in terms of better health, education, economic stability, and better quality of life. We need to find a balance that allows for the free flow of information while protecting sensitive information, based on the societal and political expectations and security needs of each country. Second, we need to avoid to the degree possible the most catastrophic consequences of the misuse of the Internet, such as damaging health and energy infrastructure, proliferating child exploitation and trafficking of women, and national security dangers. This means creating red lines that everyone can rally around. Third, we need to ensure that cyber warfare does not inadvertently lead to kinetic warfare (including nuclear) through miscalculation or misattribution of the attacks. Finally, as we craft polity, we need to keep an eye on the importance of the Internet for society and understand the risks to the societal gains if we do not reach a global consensus on cyber warfare and limit the proliferation of cyber weapons.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

About the Author

Sanjay Goel is an Associate Professor in the Information Technology Management Department (School of Business) at the University at Albany, SUNY and Director of Research at the New York State Center for Information Forensics and Assurance at the University. Dr. Goel received his Ph.D. in Mechanical Engineering in 1999 from Rensselaer Polytechnic Institute. His current research interests include information security and privacy behavior, innovative education and pedagogy, security models, i.e., biological models, risk models, and security policies and cyberwarfare. He conducts research on forensics and cybercrime, and critical infrastructures, including privacy in smart grid data analytics; the impact of security and terrorism on financial markets; resilient transportation; and resilient service-oriented architectures. *E-mail*: goel@albany.edu.