EVALUATING NUCLEAR SECURITY IMPLICATIONS OF THE SPLINTERNET

L. GEHRIG
E. BACHHUBER
R. GOYCHAYEV
Pacific Northwest National Laboratory
Richland, Washington, USA
Email: lindsey.gehrig@pnnl.gov

Abstract

The internet, which for years has been viewed as a “global online commons” with standardized protocols but few regulations is, according to some experts, starting to mirror the contentious political and commercial contours of the physical world. Contributing to this is the rise in data breaches, cyber-enabled attacks on critical infrastructure, government surveillance operations, theft of intellectual property, manipulation of electoral processes, and perceived erosion of privacy, all of which are resulting in a growing scepticism that an open internet will naturally serve the best interests of users, communities, countries, and the global economy. In addition, the rapidly emerging and increasingly lucrative power of data has global superpowers scrambling to protect their informational sovereignty as an urgent matter of national security. Underscoring this urgency is the fact that, despite its global reach and cosmopolitan contributor base, internet infrastructure and governance of the World Wide Web remain largely under U.S. corporate auspices, which reinforces the perception of U.S. control.

Whether fragmentation is politically, economically, or socially motivated, there appears to be a growing appetite for an internet that is partitioned and controlled at the national level. From “the Great Firewall of China” to the “Halal” internet of Iran, the trend towards a “Splinternet” has courts and governments embarking on what some call a "legal arms race" to impose a maze of national or regional rules, often conflicting, in the digital realm. The paper explores the emerging Splinternet phenomenon, analyses the implications of this trend on nuclear security, and identifies questions that present opportunities for future research.

1. INTRODUCTION

Since its inception nearly 50 years ago, the internet has grown significantly and has become increasingly complex. And yet, throughout its evolution, the internet has maintained several fundamental characteristics. Notably, that it is available, open, and global in nature.

However, over the past several years, a new phenomenon has emerged that is challenging the notion that the internet is a “global commons” that quickly and indiscriminately connects all corners of the world. Specifically, state governments are taking a variety of measures to control access to content and to influence—both physically and electronically—how information flows across their borders. As a result, some experts have observed that the internet is beginning to fracture into smaller enclaves that are separated by national and geopolitical borders [1]. The impetus for national control varies from state to state, but broadly speaking, motivations can be summarized as economic, political, cultural, or some combination thereof. Regardless of intent, the result has been the rise of nationally managed and fragmented internets, referred to as the “Splinternet.”

The Splinternet manifests itself differently in various corners of the world depending on the resources, capabilities, and motivations of the state involved. After discussing motivations for the Splinternet phenomenon in section 2, case studies from various countries will be examined in section 3. From this analysis we conclude the Splinternet can have both positive and negative implications for nuclear security and the broader non-proliferation regime, which are discussed in section 4. We conclude by summarizing key findings and posing additional questions that may warrant further research.

2. RISE OF THE SPLINTERNET

In the late 1960s, the Advanced Research Projects Agency within the U.S. Department of Defence initiated a research program to connect entities working on military technologies through a new computer-based communication network. This program, known as ARPANET, linked government agencies, government contractors, and universities and was the precursor to the internet [2].

As we know, the internet has grown significantly and become increasingly complex. Originally used by just a handful of academic researchers in the United States, it is now global in scale and connects nearly half of the world's population. According to one United Nations study, 3.5 billion people were using the Internet by the end of 2016, up from 3.2 billion from the previous year [3]. This connectivity is made possible through a global system of interconnected networks that are underpinned by physical hardware and administered by standardized protocols or a set of rules governing the format of data sent over the internet or other network.

For much of the world's population, the internet is now ubiquitous and deeply entwined in nearly all aspects of daily life. The public and private sectors are inextricably linked as the internet affects economic, technical, regulatory, political, and social interests. As one expert observes, "in less than two decades, the internet has evolved from an opt-in service, where citizens and governments were able to choose whether or not to participate in the internet society, to a compelled infrastructure that requires participation in order to reap its benefits and deliver essential services to citizens" [4]. This evolution has, in turn, changed public opinion regarding what citizens should have the right and privilege to access online. As corporations, citizens, governments, and non-state actors look for ways to advance their respective interests through the same platform, it becomes clear that they often have conflicting ideas about if and how the internet should be used and regulated.

Further complicating matters is the shifting perception over who has control and governance of the internet and its underlying infrastructure. Since the internet was created in the United States, and many U.S. companies (e.g., Google, Amazon, Microsoft, eBay, Apple, Facebook, Twitter, and Netflix) dominate the Information Communications Technology (ICT) marketplace, many states feel there has been a disproportionate accumulation of wealth and corporate influence in the West [4]. There is also growing concern about U.S. companies collecting and potentially exploiting consumer information. Many of the aforementioned companies provide low-cost services, such as file storage and photo sharing. By using their services, users consent to the compilation of sensitive personal data, including photos, search history, and purchasing decisions. This information is used to create behavioural prediction models and targeted advertising for commercial gain. This practice has been described by some as "surveillance capitalism" and has allowed these technology pioneers to create effective monopolies over social media, news, email, and other services [1]. The centralization of user data and its exploitation for commercial gain has prompted some countries to pursue "information sovereignty" through various state-led efforts.

Information sovereignty is not the only form of sovereignty complicated by the ubiquity of the internet. There are indeed implications beyond political control and economic growth since military operations, weapons systems, and critical infrastructure protection also depend on having an internet connection that is accessible, secure, resilient, and stable. As a result, market control of ICT commodities and services, including those used within the military industrial complex, as well as the ability to influence the debate over internet governance has become increasingly intertwined with our traditional understandings of national security and stability.

Another prevailing theme is trust, or lack thereof, in the internet-enabled activities of corporations and governments. Public trust sharply declined in June 2013 when intelligence contractor Edward Snowden leaked classified documents from the U.S. National Security Agency. In doing so he revealed the existence of a complex global telecommunications surveillance system [1] and the widespread practice of government-led data harvesting, storage, and analysis of all foreign internet traffic crossing U.S. borders, which enabled full access to user data [5].

These data were accessible to the U.S. government because a large part of the infrastructure was made or maintained by U.S. companies and most of the infrastructure was physically located in the United States.

This interconnected collection of interests and insecurities and the desire for control is inherently multilateral, multi-stakeholder, and multicultural. In order to prepare for, understand, and influence the impacts of the internet in their favour, states have responded in a variety of ways. The result has been the rise of the Splinternet.

3. WHERE IS THE SPLINTERNET HAPPENING?

The Splinternet phenomenon, where states are taking steps to control the internet—both physically and electronically—at the national level manifests itself differently in various corners of the world depending on the resources, capabilities, and motivations of the state involved. Consequently, no two examples are identical, so it is important to think about the Splinternet on a spectrum. For example, on one end we see states choosing to indigenously develop physical infrastructure and a separate but parallel architecture to support their own internet. This includes efforts to locally develop and manufacture hardware such as severs and laying separate fibre optic cables (in some cases oceanic data cables) to get around U.S. surveillance and completely firewall themselves from the rest of the world. The goal with this approach is to increase national security by mitigating threats from external networks, increase confidentiality, and improve privacy. On the other end of the spectrum, rather than building a new physical infrastructure, some states are implementing technical measures to control internet use and services by blocking access to foreign websites or requesting that U.S. companies allow them to store their citizens' data in their own country (i.e. Russian Facebook data is stored on Facebook servers located in Russia). Still further on the spectrum, some states are taking legislative or regulatory actions to achieve the same control. One of the main goals with these approaches is to preserve domestic cultural values and political control by insulating their populace from content that is perceived to be detrimental to social stability.

Below are notable examples of efforts from China, Iran, Russia, the European Union, and the United States to increase national control over the internet or implement measures to become more insulated from the World Wide Web. This list is not exhaustive but does illustrate the notion that the Splinternet exists on a spectrum and that this phenomenon is appearing in states from West to East with all manners of governance.

3.1. China: Firewall Splinternet

China maintains a domestic internet that is controlled by the Chinese Communist Party. China's internet is not completely separated from the rest of the world but access to and from it is highly controlled through a "Great Firewall," which was established in 1999 to control the spread of information undesirable to the Chinese government. The Great Firewall was established relatively early in the evolution of the internet, which enabled it to maintain control of its domestic architecture as communication infrastructure grew globally. Maintaining control of its domestic internet is also possible because all service providers in China are licensed and controlled by the state. In addition, there are only a handful of fibre optic cable companies that control access points to the internet backbone, all of whom are fully compliant with Chinese state requirements.

China has also successfully enforced regulations that limit the ability of U.S. web service companies to operate within its borders. China's internet is one without Twitter, Instagram, Pinterest, and YouTube. Large U.S. social media companies like Facebook are banned and Google shut down its search engine in China in 2010 after refusing to comply with state-mandated censorship laws. These restrictions have allowed China to develop a large domestic web service industry and, as a result, the overwhelming majority of the Chinese population uses Chinese-controlled services such as search engines and e-commerce sites.

3.2. Iran: A Splinternet of Indigenously Developed Infrastructure

Since 2012, Iran has been working to build its own national internet that is entirely separate and distinct from the global internet. The Splinternet in Iran is often unofficially referred to as the “halal” internet but formally known as the Iran National Information Network (ININ). In May 2019, Iranian state media cited government officials as saying the ININ system was 80% complete [6]. Unlike China, ININ does not just use a great firewall to block undesirable sites but has independent infrastructure to support the network, including fibre optic cables, servers, and data centres. ININ is a locally controlled version of the internet that prevents outside material and services deemed undesirable from getting into the closed system. Overall, ININ is intended to promote Islamic content while restricting what the public can see and allowing access only to what Iranian authorities view as moral. Iran has been able to create the ININ network because a state-owned firm manages all of Iran’s telecommunications and supporting infrastructure. This single point of control has enabled Iranian authorities to block certain internet services, such as Facebook, and slow down access when it is determined to be in the national interest to do so. In addition to controlling the flow of information, ININ has other reported benefits. According to Iranian authorities, the domestic economy has been boosted by efforts to build and fortify an Iranian cyber industry since the only applications and software permitted on ININ are those created in Iran [7].

3.3. Russia: Technical and Regulatory Approaches to Splinternet

Unlike Iran, Russia has not created its own independent internet and supporting infrastructure but has taken a number of steps to limit access within its borders and has essentially outlawed online anonymity and private communications. In 2012, the Russian government began restricting web users from accessing certain websites and developed a comprehensive list of banned Uniform Resource Locators (or URLs), which are unique identifiers to locate a resource on the Internet. In July 2017, Russia banned the use of internet proxy services, including virtual private networks (VPNs), which could be used to circumvent state-sponsored initiatives to control access to content. In 2019, Russia passed legislation to create its own government-controlled alternative Domain Name System (DNS). Specifically, the law requires internet service providers to disconnect from any foreign servers and rely on Russia's DNS instead, which is controlled by the Russian internet and media regulator Roscomnadzor. The bill is scheduled to go into force on November 1, 2019 and mandates that Russian internet providers encourage independence in the case of foreign aggression.

If successfully implemented, this bill would provide central control of all internet traffic and remove the need for data to be sent to and received from overseas servers. In addition to passing legislation, Russia has taken other actions to restrict the flow of information, including collaboration with the Chinese government to obtain information about internet filtering practices used in China’s Great Firewall. When thinking about the spectrum of ways to exert national influence, Russia has used a combination of legislative actions and filtering technologies to implement its version of the Splinternet.

3.4. European Union: Proposed Regional Splinternet and Legislatively Driven Control

In February 2014, German Chancellor Angela Merkel called for a closed, European-wide computing network and for national data to be stored on local servers. At that time, she said “We’ll talk to France about how we can maintain a high level of data protection…(and) about European providers that offer security for our citizens, so that one shouldn’t have to send e-mails and other information across the Atlantic” [5]. Merkel’s statement suggests she was advocating for the European Union (EU) to have its own regional internet tied to the political bloc that would be controlled separately from the World Wide Web. To date, a European-wide internet has not materialized, but this is indicative of the trend to increase national, or in this case, regional control over the internet and its underlying infrastructure.

In addition, the EU passed the General Data Privacy Regulation (GDPR) in 2018, which forces companies doing business with EU-based entities to request permission before collecting their data or face severe financial penalties. Not every company was able to comply with the EU law (at least in the short term), so some companies have resorted to geo-blocking EU customers (i.e. blocking content based on users Internet Protocol address) from their services to avoid fines. This is significant for two reasons: first, smaller companies are at a potential disadvantage as they grapple to comply with the new regulation and potentially lose customers from a large pool of consumers; second, EU residents can, as a result of geo-blocking, potentially lose access to the content and services provided by smaller companies who are working to comply with the new EU requirements. Uneven content accessibility and varying degrees of national regulation contribute to the Splinternet phenomenon, even if temporarily. Furthermore, large ICT companies have been hit by large fines as some have been slow to implement GDPR requirements. For instance, in January 2019, the French data protection authority announced that it had fined Google about $57 million for not properly disclosing to users how data was collected through its search engine, Google Maps, and YouTube [8]. The EU's enactment of GDPR is significant. While it has established policies to protect the data privacy of European citizens, it may impede the flow of international commerce and introduce a degree of variability to the online user experience that has not been seen before.

On the whole, the EU's legislative actions to establish privacy protections illustrate how states are attempting to control certain aspects of the internet. Specifically, the EU legislative and regulatory measures are indicative of the fact that citizens and the governments who represent them have lost trust in the ability of large corporations to protect their personal and financial data. They are also attempting to regain control from Western ICT firms that engage in targeted advertising and that may commercially exploit European user data. The EU's actions are focused on data privacy regulations to limit U.S. control and hegemony of the internet and are at the opposite side of the Splinternet spectrum from Iran, for example, which controls the internet through both regulations and physical development of its national infrastructure.

3.5. United States: A Regulatory Driven Splinternet

Unlike the EU, the United States has not publicly discussed plans to fragment the internet but has taken regulatory steps to limit access and content. One example of this occurred in 2018 when the U.S. Federal Communications Commission (FCC) voted to repeal consumer protections for net neutrality, which is a principle that all internet traffic should be treated equally. The 2018 ruling reversed the FCC's net neutrality order in 2015 that prevented internet service providers from blocking, slowing down, or speeding up access to online content in the United States.

With the repeal of net neutrality, U.S. service providers can now theoretically throttle or block competing content from being transmitted throughout the United States as well as content coming from other countries that is traveling via U.S. infrastructure. The impact is uneven content accessibility for customers, both domestically and internationally.

Some believe the FCC ruling may be the catalyst for a future U.S. Splinternet [9]. The FCC's rulings to limit the internet through regulation are at the opposite side of the Splinternet spectrum from Iran, for example, which has taken both steps to implement regulations and build its infrastructure backbone in support of its Splinternet.

3.6. Internet Freedom and Broader Internet Censorship

The issue of content accessibility is pervasive globally as many countries censor content on the internet for different reasons. For example, North Korea blocks all outside traffic online and its internet consists of roughly two dozen websites [10]. South Korea, on the other hand, blocks almost one thousand websites within its borders due to what it views as culturally offensive content [11]. Other countries such as Burma, Saudi Arabia, Syria, Egypt, and Vietnam restrict political speech through censorship and monitoring practices. According to a 2018 report by Freedom

House, a research organization that is partially funded by the U.S. government, states are exerting increased control over internet traffic within their borders to insulate themselves from the outside and as a result, “freedom of the Internet” has declined for eight consecutive years” [12]. The point here is not to make a value judgement on censorship, but to point out that the type and amount of information available online is compelling states to gain or regain control of what is viewed online.

Overall, the growing Splinternet phenomenon is the result of concerns about the impact of the global internet on diverse economic and political institutions, cultural values, and the desire to defend cyber borders from actors and ideas that present a threat to national security and power. The Splinternet phenomenon gains momentum from structural changes, technical measures, and regulatory actions that are instituted at the national or regional level.

4. IMPLICATIONS FOR NUCLEAR SECURITY AND NONPROLIFERATION

The impact of the Splinternet on nuclear security has not been extensively examined. However, based on current observable trends and what is known about the integration of digital systems into nuclear facilities, it is plausible that a fractured, nationalized internet infrastructure and associated communication protocols will yield both positive and negative outcomes.

According to the International Atomic Energy Agency (IAEA), “The pervasive presence and use of computer-based systems associated with a nuclear facility, throughout the facility’s lifetime, makes it likely that computer-based systems will be used to perform or support the majority of key tasks and activities related to facility functions” [13]. Computers, computing systems, physical protection systems, instrumentation and control systems, and other digital components play an increasingly important role in the management of sensitive information, nuclear safety, nuclear security, and material accountancy and control at nuclear facilities [14]. While the incorporation of computer-based systems has enhanced system performance and improved efficiencies, it has also changed the number and nature of risks to the facilities themselves. These risks are, at least in part, determined by how computer-based systems send and receive information. Herein lies the potential for the Splinternet to be viewed as a positive phenomenon for nuclear security.

4.1. Splinternet Would be Good for Nuclear Security

If the computer security of nuclear facilities is the only variable being evaluated for positive or negative Splinternet implications (as opposed to social and economic implications), it stands to reason that a nuclear facility within the territory of a country whose national internet is physically separated from the open web would be more secure against a certain range of threats, since separation makes it significantly more difficult for a foreign country to launch a cyber-attack without physical access. We recognize that the physical separation of infrastructure is only one of several examples along the spectrum of Splinternets, but it is the most extreme and thus worthy of exploration should the phenomenon continue to grow in scope and intensity.

The notion of keeping critical facilities physically separated from the open internet was emphasized in a 2017 study by the U.S. President’s National Infrastructure Advisory Council (NIAC) [15]. The U.S. National Security Council asked the NIAC to examine how U.S. federal authorities and capabilities can best be applied to support cybersecurity of high-risk assets, particularly in the electric and financial sectors. The first recommendation from the NIAC report was to establish a separate, secure communications network specifically designated for the most critical cyber networks. The NIAC encouraged the National Security Council to undertake a pilot project that would create a dedicated communication network for critical infrastructure sectors to demonstrate the ability for pilot organizations to operate critical control systems in isolation from public networks, making them more difficult to access and thus less vulnerable to cyber-attacks.

Short of building an entirely separate communication network, facilities may choose to adopt other measures such as analogue technology or manual controls in order to increase their security posture. In the United States, this notion is not far-fetched. In June 2019, the U.S. Senate passed the Securing Energy Infrastructure Act, which is aimed at removing vulnerabilities that could allow hackers to access the energy grid through holes in digital software systems [16]. The bill is intended to isolate and defend industrial control systems from security vulnerabilities by incorporating analogue and nondigital control systems, purpose-built control systems, and physical controls. Press releases related to the bill state that, "This approach seeks to thwart even the most sophisticated cyber-adversaries who, if they are intent on accessing the grid, would have to actually physically touch the equipment, thereby making cyber-attacks much more difficult" [17]. While the focus of this particular bill was on the energy grid, the same logic applies to nuclear facilities.

There are, however, downsides to analogue technology and manual controls. Chris Doman, security researcher at AT&T Alien Labs, told Forbes magazine that, "Requiring a certain amount of manual operation as standard may be a good way of truly enforcing an air-gapped[1] system [but] it can be very hard to ensure there are no automated workarounds" [18]. He further added his concerns regarding the financial impacts associated with manual controls, which would not only affect the efficiency of operations but would also have consequences with respect to human capital development as they would require a deep cadre of sufficiently trained, qualified, and experienced staff to take control in the event of a system failure [18].

The Splinternet would not require analogue technology or investments in human capital development to make nuclear facilities more secure. By virtue of being on a separate and distinct national internet with cables, servers, and data centres completely severed from the global Internet, the security posture of a given facility would be inherently more robust. In October 2018, the American business magazine Fast Company, which focuses on technology, business, and design, explored the Splinternet phenomenon and concurred that "[…] if a country's economic or defence or transportation infrastructure was not on the same internet as the foreign superpower, it would be infinitely harder for that more advanced security threat to access the proverbial pipes it needs to carry out its attacks" [5].

If we can agree that a nuclear facility within the territory of a country whose national internet is physically separated from the open web would be more secure, does this mean that Splinternets are a worthwhile undertaking to promote nuclear security?

4.2. More to Nuclear Security than Splinternet

It is important to acknowledge the significant number of nuclear security threats and attack vectors that are essentially agnostic to internet connectivity and configuration. Within the cyber domain, there are examples of malicious attacks on nuclear facilities that utilized malware and other exploits without leveraging the internet; they all spread via local area networks [19]. In addition, the Splinternet could reduce cyber security at a facility if, for example, software updates and threat information were unable to be shared between facilities in different countries.

Outside of the cyber domain, there are several elements essential to comprehensive nuclear security that would remain essential regardless of whether or not a given state pursued a Splinternet. The essential elements include but are not limited to robust physical protection, capabilities to prevent sabotage, insider threat mitigation, nuclear material accounting and control, supply chain risk management, and defence strategies for blended attack scenarios. The importance and potential impacts of these nuclear security elements have been broadly recognized by the international community and an in-depth analysis is outside the scope of this study. However, it is reasonable to conclude that while

[1] An air-gapped computer is one that is neither connected to the internet nor connected to other systems that are connected to the internet.

a national internet that is physically separated from the open web would make a nuclear facility more secure from cyber-attacks, it would not be a remedy for the other myriad and complex risks necessary to secure nuclear facilities.

Not only is the Splinternet far from a panacea, the very phenomenon has broader implications beyond nuclear security and presents challenges to some of the fundamental underpinnings of the non-proliferation regime.

4.3. Treaty Verification

The Comprehensive Nuclear Test Ban Treaty (CTBT) is a multilateral treaty that bans all nuclear explosions, for both civilian and military purposes, in all environments, on the Earth's surface, in the atmosphere, underwater, and underground. As part of the CTBT verification regime, the International Monitoring System (IMS) is used around the world to detect signs of nuclear explosions by using seismic, hydroacoustic, infrasound, and radionuclide monitoring capabilities. With over 325 facilities globally, IMS stations depend on a well-functioning communication system for the timely, reliable, and accurate transmission of data in near-real time to the International Data Centre in Vienna where data are processed and analysed.

Understanding the volume of data being transmitted helps underscore why worldwide connectivity is so fundamental to the CTBT verification regime. According to the CTBT Organization, "…35 gigabytes of data are being transmitted every single day, either coming from monitoring stations or being sent to Member State national data centres" [20].

Although satellite-based communication is used for the bulk of data transmission, the CTBT verification regime also utilizes VPN technology that makes use of public telecommunication infrastructure, like the internet, to connect outside users to an organization's network. Several IMS stations rely on VPNs to communicate out of necessity, as the satellite-based structure is not feasible in their remote locations. Without confidence that data will be transmitted securely and reliably through a complex network of land-based and satellite connections, the international community's trust and confidence in the global commitment to ban nuclear explosion testing will be significantly undermined.

Should the Splinternet phenomenon lead to nationally managed and fractured internets that communicate (or do not) using diverse protocols and standards, it could inhibit or prevent the secure and timely transmission of detailed IMS data that enables Member States to assume their rights and fulfil their responsibilities under the CTBT.

4.4. International Safeguards

Due to the evolving nature of cyber threats, as well as the increasing level of sophistication of safeguards processes and procedures, the international safeguards regime is increasingly interconnected and thus vulnerable to disruption and manipulation from computer-based security threats. Given this interconnectivity, when it comes to the Splinternet, potential disruption to the safeguards regime exists not only because of the instrumentation at nuclear facilities, but also because of impacts the Splinternet would have on the collection and transmission of safeguards information, which is essential for Member States to provide assurances to the IAEA and to one another about their nuclear material and nuclear programs.

4.4.1. Instrumentation

The IAEA relies heavily on the ability to transmit data from unattended monitoring and surveillance systems installed in nuclear facilities back to their headquarters in Vienna or to their field offices in Tokyo or Toronto. These systems are comprised of video cameras, radiation detectors, sensors, and seals, all of which provide information to the IAEA and thus assurances to the international community regarding activities at safeguarded facilities. As of 2016

there were over a million pieces of encrypted safeguards data collected by over 1,400 surveillance cameras and 400 radiation or other sensors installed around the world [21].

The cost of physical inspections and equipment maintenance of this monitoring and surveillance equipment is significant, so by accessing these systems remotely to perform maintenance such as software upgrades and configuration settings, the IAEA saves costs and gains efficiencies. This is an appealing option to a budget-constrained agency. To be sure, unattended and remote monitoring remains one of the most efficient ways to provide up to date safeguards information for evaluation by inspectors while maintaining state of health status on the equipment. At the same time, remote access increases the potential opportunity for someone to hack into these systems, placing the authentication of the data and configurations of these systems at risk.

4.4.2. Safeguards Information

Beyond data transmission from equipment, the Splinternet could pose further complications to the safeguards regime with respect to Member State reporting. There are several examples of safeguards information that is sent to the IAEA over the internet, including nuclear material accountancy data, Additional Protocol reporting, and inventory change reports. In each of these examples, the confidentiality, integrity, and availability of the information from Member States to the IAEA is supremely important. If the Splinternet phenomenon evolves to a point where safeguards data, whether from instrumentation or reporting requirements, needs to navigate a system of fractured, nationalized internets in order to be transmitted to the IAEA headquarters in Vienna, there could be significant technical challenges and political resistance. Without trust and confidence in the origin and integrity of the information used as the basis for drawing safeguards conclusions, there will not be trust and confidence in the overall safeguards regime.

5. CONCLUSIONS AND FUTURE CHALLENGES

The paper explored the emerging Splinternet phenomenon, analysed implications of this trend on nuclear security, and identified policy questions that present opportunities for future research. The key takeaways of this study are:

- There are indications that the internet is fracturing into smaller enclaves that are separated by national and geopolitical borders. This phenomenon has been referred to as the Splinternet.
- The impetus for the Splinternet varies from state to state, but broadly speaking, motivations can be summarized as economic, political, cultural, or some combination thereof.
- There are several notable examples of states that have implemented their own Splinternet or are considering such a move. This includes Western and non-Western states.
- The Splinternet phenomenon gains momentum from structural changes, technical measures, and regulatory actions that are instituted at the national or regional level.
- The Splinternet presents both positive and negative potential implications for nuclear security.

Questions for further research may include:

- Will the Splinternet lead to disparate efforts to monitor malware threats and, as a result, increase the severity of malware outbreaks or will distributed monitoring with an increased focus on national interests lead to positive outcomes?
- How will the international community maintain confidence in the non-proliferation regimes that depend on sending and receiving data from all corners of the globe if new protocols and information sharing arrangements have to be established?
- Will it be more difficult to provide robust configuration management across unique application domains?

— What are the safety and security implications for industrial control systems (PLCs and similar) if they become less standardized?

It is our hope that this study raises awareness about the Splinternet phenomenon and encourages additional research on its impacts for nuclear security. Depending on how the phenomenon continues to evolve, policy and technical solutions may be called for to ensure the world maintains confidence in the treaties, security measures, verification regimes, and institutions that comprise the international non-proliferation regime in the era of Splinternet.

REFERENCES

[1] SKYCOIN, Cyberbalkanization and the Future of the Internets, accessed 14 October 2019, https:/medium.com/skycoin/cyberbalkanization-and-the-future-of-the-internets-f03f2b590c39.

[2] DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, Paving the Way to the Modern Internet, accessed 17 October 2019, https:/www.darpa.mil/about-us/timeline/modern-internet.

[3] UN NEWS, Nearly 47 Percent of Global Population Now Online – UN Report," 2016, https:/news.un.org/en/story/2016/09/539112-nearly-47-cent-global-population-now-online-un-report.

[4] HATHAWAY, M.E., Connected Choices: How the Internet Is Challenging Sovereign Decisions," American Foreign Policy Interests, Volume 36, Number 5, 2014.

[5] GROTHAUS, M., Get Ready for the Splinternet: The web might not be worldwide much longer, Fast Company, 2018, https:/www.fastcompany.com/90229453/get-ready-for-the-splinternet-the-web-might-not-be-worldwide-much-longer.

[6] SHERMAN, J., Russia and Iran Plan to Fundamentally Isolate the Internet, Wired, 2019, https:/www.wired.com/story/russia-and-iran-plan-to-fundamentally-isolate-the-internet/.

[7] RHOADS, C., FASSIHI, F., Iran Vows to Unplug Internet, Wall Street Journal, 2011, https:/www.wsj.com/articles/SB10001424052748704889404576277391449002016.

[8] SATARIANO, A., Google is Fined $57 Million under Europe's Data Privacy Law, New York Times, 2019, https:/www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html.

[9] COREN, M.J., What will happen now that net neutrality is gone? We asked the experts. Quartz, 2017, https:/qz.com/1158328/what-will-happen-now-that-net-neutrality-is-gone-we-asked-the-experts/.

[10] MCGOOGAN, C., North Korea's Internet Revealed to Have Just 28 Websites, The Telegraph, 2016, https:/www.telegraph.co.uk/technology/2016/09/21/north-koreas-internet-revealed-to-have-just-28-websites/.

[11] VOLODZKO, D., Is South Korea Sliding Toward Digital Dictatorship? Forbes, 2019, https:/www.forbes.com/sites/davidvolodzko/2019/02/25/is-south-korea-sliding-toward-digital-dictatorship/#29dd77f3648e.

[12] FREEDOM HOUSE, Freedom on the Net, accessed 14 October 2019, https:/freedomhouse.org/report/freedom-net/freedom-net-2018.

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, Draft Technical Guidance, pg. 26, IAEA NST-047, Vienna, Austria, 2017.

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Conducting Computer Security Assessments at Nuclear Facilities, IAEA TDL-006, Vienna, Austria, 2016.

[15] NATIONAL INFRASTRUCTURE ADVISORY COUNCIL, Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure, 2017, https:/www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf.

[16] U.S. CONGRESS, Securing Energy Infrastructure Act (S 174, 116th Congress), 2019, https:/www.congress.*gov*/116/bills/s174/BILLS-116s174rs.pdf.

[17] U.S. SENATOR ANGUS KING, Senate Passes King Bill Protecting Energy Grid from cyber-attacks, 2019, https:/www.king.senate.gov/newsroom/press-releases/senate-passes-king-bill-protecting-energy-grid-from-cyber-attacks.

[18] O'FLAHERTY, K., U.S. Government Makes Surprise Move To Secure Power Grid From Cyberattacks, Forbes, 2019, https:/www.forbes.com/sites/kateoflahertyuk/2019/07/03/u-s-government-makes-surprise-move-to-secure-power-grid-from-cyber-attacks/#14488f383191.

[19] ZETTER, K., "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," Wired Magazine, 2011, https:/www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

[20] COMPREHENSIVE TEST BAN TREATY ORGANIZATION, The Global Communications Infrastructure, accessed November 2019, https:/www.ctbto.org/verification-regime/the-global-communications-infrastructure.

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Surveying Safeguarded Material 24/7, Vienna, Austria, 2016, https:/www.iaea.org/newscenter/news/surveying-safeguarded-material-24/7, September 2016.