International Journal of Korean Unification Studies
Vol. 25, No. 2, 2016, 77–103

The Deficiencies of a Westphalian Model for Cyberspace: A Case Study of South Korean Cyber Security

Gus Swanda

Viewing contemporary attempts of technologically-advanced countries to restrict outsider access to critical websites and infrastructure through the lens of the 1648 Treaty of Westphalia, there has been significantly more credence given to the idea that nation-states are moving towards creating an infrastructure for national cyber borders. If successful, such a model would create new economic, social and technical problems that may pose greater threats to national security. This paper explains the drawbacks of the cyber-Westphalian model using South Korean cyber policy as a case study, and highlights the potential dangers of restricting the internet at the national level. Through data collected from South Korean computer users and secondary sources, the author finds that the implementation of national borders in cyberspace is not feasible. In addition, such a model would bring with it severe detriments to the online economy and personal freedoms, while still leaving vital systems vulnerable.

Keywords: South Korean Cybersecurity, Cyber Borders, Cyber Westphalia, Cyber Policy, Cyber Defense

Cyberspace has become the central nervous system of nations' communications, government and commercial operations, infrastructure and security. As the internet grew in scale, so too did the dependence on cyberspace and vulnerability to cyberattack. The fear that a person, group or rival state could inflict catastrophic damage to a nation through the internet has put national cybersecurity at the forefront of

* This work was supported by the research grant of the Busan University of Foreign Studies in 2016.

debates on security policy. Malicious codes such as Stuxnet have shown that all systems, both online and offline, are potentially vulnerable to destruction. Some scholars posit the eventual outcome of the current dynamic is the construction of national borders within cyberspace.[1] As this national strategy becomes more prolific, cyberspace will begin to resemble the current real-world, Westphalian border system.[2]

This paper examines the cyber-Westphalian model and poses several central questions. First, are borders in cyberspace a fait accompli? Second, are virtual borders technologically possible, psychologically comfortable, and systemically and politically manageable, as the theory purports? Lastly, what are the potential detriments to nations that pursue and/or achieve such sovereignty over their national cyberspace? To answer these questions, the author analyzes the work of Chris C. Demchak and Peter Dombrowski on cyber borders. Due to South Korea's status as a democratic and industrialized nation with an advanced and ensconced high-speed cyber infrastructure, and its efforts towards a relatively closed and nationalized internet, the author uses South Korean cybersecurity policy and its management of national cyberspace as a case study. Key aspects in the organization, execution and monitoring of its national internet are essential for creating borders in cyberspace, and therefore the conclusions drawn from the South Korean exemplar are applicable to other countries seeking to create national borders in cyberspace. It is concluded that cyber borders, such as those proposed by Demchak and Dombrowski, are not inevitable. Although virtual borders may be technologically pos-

1. Holcomb Lee, and Shrewsbury June, "Securing Our Cyber Borders," *Innovation* 9, no. 1 (February/March 2011), http://www.innovation-america.org/securing-our-cyber-borders (accessed January 14, 2016). Also see Katherine Maher, "Cybersecurity: 'The New Westphalian Web'," *Truman National Security Project Doctrine Blog*, February 25, 2013, http://trumanproject.org/doctrine-blog/cybersecurity-the-new-westphalian-web/ (accessed August 14, 2016).
2. The Peace of Westphalia was a series of peace treaties signed between May and October 1648 in the Westphalian cities of Osnabrück and Münster that ended several European religious wars. These treaties were the first to recognize the authority of diplomatic congress, and establish the modern concept of the sovereign state in Europe.

sible, they are not necessarily feasible, nor are they always psychologically comfortable nor systemically and politically manageable. Furthermore, the economic and social costs of pursuing such a model make it unlikely that liberal democratic, developed nations will fully adopt it.

National Borders in Cyberspace

Chris C. Demchak and Peter Dombrowski state in their paper, "Rise of a Cybered Westphalia," that the relatively ungoverned frontier of cyberspace, like all frontiers, does not last forever where human societies are involved. Eventually, nation-states will extend their sovereignty to the internet and exert control over the electronic information that comes in and out of their domains, and in essence create electronic borders. Demchack and Dombrowski cite the recent developments in the cybersecurity policies of developed nations as evidence that states are already moving towards a bordered internet.[3]

According to Demchak and Dombrowski, "the transformation from frontier to substrate across cyberspace" began with the discovery of the Stuxnet virus in 2010. Stuxnet was a virus planted in the systems of Iran's nuclear centrifuge. It eventually destroyed those systems and set the Iranian nuclear program back years. The malicious software was believed to be uploaded to the secure, Iranian off-line system via USB flash drives. Ingeniously crafted, the virus employed many new sophisticated techniques and codes that were designed with specific knowledge of its target. Such an endeavor required the resources of an advanced country with an extensive intelligence network, and have led some to believe that it was created by the United States, Israel or both.[4]

---

3. Chris Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 6 (2011), pp. 32, 34-35.
4. Kim Zetter, "Stuxnet Attack on Iran Was Illegal 'Act of Force'," *Wired*, March 25, 2013, https://www.wired.com/2013/03/stuxnet-act-of-force/ (accessed June 13, 2016).

Without remote directions, Stuxnet meticulously sought and destroyed a predetermined section of the centrifuge and demonstrated that heavily secured systems not connected to cyberspace are still vulnerable to cyberattack. For Demchack and Dombrowski, this was a turning point in cybersecurity policy. Developed nations now had a concrete example of a cyber threat with real-world catastrophic potential. More importantly, nations now have a reason to draw lines and establish sovereignty over the internet.

Demchack and Dombrowski maintain that the response will be to move further towards a closed, bordered internet system that can more thoroughly scrutinize foreign data and thereby prevent potential threats to national security.[5] Examples of how states are already administering such cybersecurity strategies are then given. According to their theory, cyberspace is no longer only under the jurisdiction of state-run communications and commercial agencies. Many industrialized nations are now treating cyberspace as another operational domain of the military. South Korea is surely another example of this. In addition, countries like China and the United States are developing technology and defensive strategies that can create such borders in cyberspace and allow nations to deal with cyber threats, even when those threats come from their own citizens.[6] These nations have already demonstrated their willingness to go on the offensive, if need be, to protect national interest. The militaries of technologically-advanced countries have engaged in cyber warfare that goes beyond simple espionage or vandalism, and seek to extend their regional and international security paradigm to the realm of cyberspace. Such actions have forced less technologically advanced countries to push their more developed allies to secure their cyberspace through traditional security arrangements and organizations such as NATO and the UN, as the cyber-Westphalian map begins to take shape.[7]

---

5. Demchak and Dombrowski, "Rise of a Cybered Westphalian Age," p. 33.
6. Swaine Michael D., "Chinese Views on Cybersecurity in Foreign Relations," *China Leadership Monitor*, September 20, 2013.
7. Demchak and Dombrowski, "Rise of a Cybered Westphalian Age," pp. 36, 48-49.

The concept of a partitioned, defined, organized and controlled cyberspace runs contrary to how most people perceive the internet. It is not a distant, sparsely populated region of the country. The frontier of cyberspace is a network of billions of systems in virtually every part of the world, with an equal number of diverse actors. The exponential acceleration of technological evolution and innovation therein has formed an environment in which the aggressors manage to outpace defensive strategies and systems. Software and hardware designed to steal information, subvert systems, disrupt public policy, and mask the user's identity are freely shared among hackers underground. Also, computer users in liberal democracies have become accustomed to the freedom that a borderless cyberspace provides. Attempts by governments to close this Pandora's box are often met with resistance that spills over into the political arena, and has a significant effect on policy. Unlike a physical frontier, reining in cyberspace would seem to be impossible. However, Demchak and Dombrowski assert that reclaiming sovereignty over the internet is technologically possible, psychologically comfortable, and systemically and politically manageable.[8]

It is further postulated that once technology is in place, states will come to military, criminal and civil agreements defining responsibility and jurisdiction in cyberspace. There have been several international civil and criminal cases involving cyberspace jurisdiction, and going forward these territorial issues will be codified through international institutions. "As civil society extends into cyberspace with rules of accepted behavior reinforced by modern state institutions, it becomes easier to invoke the routine activities of international organizations to curb, if not cure, the disruptive activities of the failed-state portions of the international virtual globe. As a result, institutions will adapt and adjust while replicating the functional aspects of the current physical concords and rules of behavior to contain the harm by actors who deviate from the emerging virtual civil world."[9]

It is Demchack and Dombrowski's contention that the new map

8. Demchak and Dombrowski, "Rise of a Cybered Westphalian Age," p. 35.
9. Ibid., pp. 44-46.

of cyberspace complete with borders, boundaries, and frontiers that are accepted by all states is inevitable. The beginnings of which can already be seen in countries such as the U.S., China, South Korea and the EU to varying degrees.[10] However, examining not only the cyber military policy of these states, but also their public and commercial internet policies reveals that it will be difficult for many liberal democratic nations to execute and enforce even basic restrictive cyber policies. Furthermore, creating cyber borders depends on a partitioning of cyberspace through technology and national public standards, and although states can have shared agendas on cybersecurity, they rarely have common standards when it comes to executing cybersecurity. Such disconnects in cyber policies within a cyber-Westphalian system would impede the flow of cyber traffic necessary for many forms of international communication and commercial interaction. Forrest Hare agrees with the basic concept of cyber borders, but cautions policy makers not to disrupt the connectivity between nations.[11] By applying Kunrether and Heal's game-theoretic approach to binary choices (known as the interdependent security investment decision) to international cybersecurity, they arrive at two conclusions. First, the probability of a state investing adequately in cybersecurity is directly related to the threat level at which it perceives cyber incursions. Secondly, in order for cyber borders to be effective, all nations must participate. Hare uses his own model for interdependent liberal democracies to show that in order for cyber borders to be effective, all relevant nations must participate.[12] The fewer states that participate, the greater the probability of a successful attack. If only one state or a few states participate, the system is compromised.[13] There

10. Demchak and Dombrowski, "Rise of a Cybered Westphalian Age," pp. 48-49, 57.
11. Forrest Hare, "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?" *School of Public Policy, George Mason University Cryptology and Information Security Series Volume 3: The Virtual Battlefield: Perspectives on Cyber warfare* (2011): 88-105, DOI: 10.3233/978-1-60750-060-5-88.
12. G. Heal and H. Kunruther, "Self-protection and Insurance with Interdependencies," *Journal of Risk and Uncertainty* 36, no. 3 (2008):, pp. 103-123.

is little or no benefit for states to construct cyber borders if they maintain a connection with allies who do not pursue such borders.[14] As the utility of the internet expands, and reliance on internet-driven communications and commerce created in a borderless cyberspace increases, states may be less inclined to participate. Thus more obstacles to cyber borders are created, making a cyber-Westphalian system less probable.

South Korea can be seen as a litmus test for liberal democracies following a closed internet strategy. It has already experienced the difficulties of limiting cyberspace from its initial forays in cybersecurity policy. In the late 1990's, the South Korean government financed the construction of the country's advanced cyber infrastructure. To protect its investment, policy makers took several steps intended to ensure that public cybersecurity protocols would be sufficient to combat most existing threats. Among these steps were the creation of the national public-key infrastructure (NPKI), and the evolution of agencies and departments responsible for monitoring cyber activities and enforcing cyber policy. As South Korean internet proliferation grew, policy began to increasingly limit anonymity, content, and access to foreign sites, and restricted e-commerce activity in an attempt to preserve the centralized security function and social integrity of its cyberspace. However, these actions had the unintended consequences of limiting the commercial potential of the internet in South Korea. This strategy may have also facilitated the theft of personal information of its citizens and ended up actually making South Korean systems more vulnerable to incursions.[15] During the past fifteen years, South Korea has been the victim of many successful large-scale attacks, and

13. Hare uses the analogy of two airplanes from different airlines, boarding at the same time. Both airlines must inspect all of their passengers' luggage. If one of the airlines fails to do so, a malicious actor may be able to plant a bomb on the secured plane through the unsecured airport.
14. Hare, "Borders in Cyberspace," 2010.
15. Keechang Kim, "Recent Changes in the Regulatory Landscape for E-Commerce in South Korea," *The Asian Business Lawyer* 16 (Fall 2015), p. 93, file:///C:/Users/user/Downloads/04.Keechang Kim_article(3).pdf (accessed December 24, 2015).

has seen its carefully laid plans to partition and defend national cyberspace begin to possibly unravel.

This paper highlights the deficiencies in the cyber-Westphalian model. As was the case with South Korea, nations who pursue borders in cyberspace will have to either drastically change the nature and scope of their plans for a nationalized cyberspace, or abandon the concept altogether. In the next section, the many obstacles to creating virtual borders are examined in greater detail. The author illustrates the potential economic consequences of partitioning the internet along national lines. Ultimately, this is a critical analysis that challenges Demchak and Dombrowski's concept of the Stuxnet attack as a catalyst for strengthening the monitoring of data flowing in from outside national borders.

Obstacles to Virtual Borders

Demchack and Dombrowski's model is predicated on the assertion that virtual borders are technologically possible in addition to being psychologically and politically manageable. However, there is evidence that suggests, for liberal democracies, this may not be the case.

Technical Impediments

Technologically speaking, there have been a number of innovations that may make borders in cyberspace possible. However, they are not without their logistical limitations. Although cyber borders may well be desired by developed nations, the implementations to such technology might make it unfeasible. Collectively, hackers have historically had an advantage over those defending national systems. Within the parameters of the current architecture of the internet, it is still not possible in some cases to detect new malicious code, locate and identify attackers or fully secure vital, offline systems. However, even if future technological advances were to allow nations to sequester their national cyber infrastructures, there still seems to be no guarantee

that such actions would make systems more secure.

Technologies for securing borders in cyberspace must be able to scan all information coming through their networks and detect malicious or illegal codes, distinguish between national and international content, and identify and locate their source. The conventional wisdom has been that such security measures are simply impossible to enforce completely, and that no defense is impenetrable. No matter what kind of defensive strategy or technologies states may devise, given enough time, every system can be hacked. Current technology cannot scan all incoming data to determine national origin and threat potential, nor can modern forensic techniques always track the source of the hack and the identity of the hacker with complete confidence.[16] Demchack and Dombrowski argue against this by suggesting that governments require data to be tagged at the source.[17]

In addition to tracking, such configurations also allow China to control its internet through three main internet gateways. They further cite China's efforts to create its own internet known as China's Next Generation Internet (CNGI). Expansion of the number of internet addresses (IPv6) allows for each machine in their cyberspace to be tagged and tracked by its own unique web address. Such a design requires a significant investment in infrastructure, but this "three-dimensional" approach allows for greater control without sacrificing the speed of the network. Such a description infers that the CNGI is secure and cannot be subverted. However, this is not entirely accurate. There are many ways around the security protocols of the CNGI.[18]

---

16. Cisco Systems, "Defending Cyber Borders: Beyond the Virtual Maginot Line," 1105 Media and Cisco GovEduTV Interactive video cast, October 25, 2012, http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/fedbiz121212maginot.pdf (accessed April 14, 2016).
17. Demchak and Dombrowski, "Rise of a Cybered Westphalian Age," p. 48.
18. Sending traffic over TCP/IP, requires both a MAC (Medium Access Control) address (e.g., 3c:12:56:88:ab:00) and an IP address (e.g., 192.168.14.5). An IP address is a logical address whereas a MAC address is a physical address. There are special devices called routers (and bridges) that connect two or more domains. Users accessing the internet through mobile computing devices will touch many different MAC networks (home, work, public internet

With enough time and investment, any technology, cyber defense strategy or internet architecture can be realized, but the question over the feasibility of such actions would remain. Cryptography covers four main areas of information security: authentication, integrity, non-repudiation, and confidentiality. Encryption can only be used to verify the sender's identity and that the message is intact. So theoretically, the technology that would allow a nation to control its own cyberspace does indeed exist. However, a bigger issue is that of public and private shared keys.[19]

Cryptography can be broken down into two broad areas: shared-key cryptography and public key cryptography. Shared key cryptography allows preselected recipients with a cryptographic key to access ciphered information. Identical private keys that are shared between the users encrypts plain text information and decrypts ciphered information. The problem with shared-key encryption is distributing the key between communicants. If one of these keys is given to the communicants via the internet, then it may be intercepted, replicated, and used to access the information by those outside the system. If one key is distributed offline, then it is vulnerable to other methods of espionage, and distribution of the key becomes more difficult as the number of participants increase. If a nation were to use this method to encrypt its national internet, distributing the key to all its citizens securely would be next to impossible. Also, shared-key encryption is vulnerable to known-plaintext attacks, chosen plaintext attacks, differential cryptanalysis, and linear cryptanalysis.[20]

---

access, etc). There are different IPv4 or IPv6 addresses at every location. Although MAC addresses are supposed to be unique to every device in the world (256^6 possible addresses), they can be hidden and replaced with a false MAC or "spoofed" (Author's interview with Jim Jackson, a Principal Software engineer at BAE systems, September 30, 2014).

19. Larry D. Bennett, "Cryptographic Services — A Brief Overview," *SANS Institute InfoSec Reading Room*, October 10, 2001, https://www.sans.org/reading-room/whitepapers/vpns/cryptographic-services-overview-749 (accessed February 13, 2016).
20. Hans Delfs and Helmut Knebl, "Symmetric-key Encryption," *Introduction to Cryptography: Principles and Applications* (Berlin, Heidelberg, New York: Springer, 2007).

Public key distribution on the other hand, allows a large number of public users access to text while at the same time verifying the identity of the communicants and ensuring that only authorized users have access to it. This system, known as a public key infrastructure (PKI), involves generating two separate keys. One key at the source (website) is private, and the other key belongs to the public user. A site that wants to be publicly accessed will request a digital certificate from server administrators. Once it receives the digital certificate, the site can now verify the digital identity of a user, and vice versa. The unique or identifying quality of each key is referred to as a digital (or electronic) signature. If web browsers were the only entity deciphering and verifying these keys, malicious users could steal the private key and access the user's information. Such hackers could also steal the public key, make a false website and access the information of multiple users. To prevent this, servers rely on a certification authority or CA. These CAs are trusted third-parties that issue a digital certificate to the site and to the users. These certificates are confirmed by the web browser, so a CA must be trusted by all of the major web browsers to allow access to all, regardless of which browser the user uses. The digital certificates are often reissued automatically at random intervals to ensure that they have not been compromised. Periodic audits are also performed on the CA by auditing companies such as WebTrust and Verisign.

In South Korea, the public key infrastructure is not administered extra-governmentally. It relies on the Korean Internet Security Agency (KISA) as a central certificate authority, and falls under the jurisdiction of the Ministry of Science, ICT and Future Planning (MSIP). Acting as the "root" CA, KISA dispenses control over the expedition of digital certificates for public and private keys to officially accredited and privately run CAs. Currently, there are five Korean companies that are accredited CAs.[21] These encryption policies in South Korea are the

21. Korea Internet Security Agency (KISA), "Public Key Authentication Service," *Public Key Authentication Service*, http://rootca.kisa.or.kr/kor/popup/foreigner_pop1_en.html (accessed February 15, 2016).

foundation for what is known as a "national public key infrastructure," or NPKI.

Political Obstacles

Given the nature of civil societies in liberal democracies, it is not entirely certain that cyber borders would be politically manageable. In some societies, freedom of expression supersedes issues of cyber security within the politic. For these countries, cyber borders would not be politically manageable. Furthermore, the democratic process in many countries often impedes the formation of the political consensus that is required to expedite new cyber policy. The speed of technological development relative to that of policy formation also makes it extremely difficult for governments to legislate technology.

The nation's earliest form of cybersecurity policy was to require all users making internet transactions to verify their identity by entering their national ID number via SEED encryption software. But doing so requires the user to run a program called 'ActiveX.' The program was designed to identify malicious code embedded in add-ons and plugins that are required to use many websites. Every time someone uses these sites, ActiveX prompts the user to verify that they know the risks involved with the download, and if they would like to proceed despite the potential danger. This policy led to the unintended consequences of requiring users to use Windows (often an older version that would run ActiveX) and Internet Explorer in order to interact with many South Korean websites.[22]

As suggested by Demchak and Dombrowski, a national control mechanism, such as South Korea's NPKI, would seem to provide greater cybersecurity. However, that has not necessarily been the case, as problems with software compatibility created new vulnerabilities with the NPKI, which can be traced to early internet policies. In 1999, the Electronic Signature Act directed all domestic websites running

22. "For World's Most Wired Country, Breaking Internet Monopoly is Hard," *Korea Times*, April 16, 2013.

embedded technologies (such as credit card or other financial transaction processing, exchange rate and measurement conversion calculators, geographical location devices, embedded database search engines, etc.) to require their users to provide proof of identity, in the form of the user's national ID number, in addition to his or her private key. It was this system that initially caused incompatibilities with web browsers, as the great number of sites with these embedded technologies could not be accessed due to the inability of most web browsers to properly generate SEED encrypted ID number verification. Fortunately for Microsoft, it had already developed ActiveX in 1996, a program that allowed browsers using its earlier binary interface standards to access these embedded technologies. The ActiveX plug-in also allowed users in South Korea to download the SEED ID verification and all embedded technologies on a Korean site.[23]

This is especially problematic from a security standpoint. Users must download the embedded programs through ActiveX, often multiple times during a single visit, each time potentially exposing their systems to malware implanted at the source or in systems with copies of Internet Explorer or Windows that have been compromised. Furthermore, these downloaded programs are deleted when the user's cache and/or temporary downloads are cleared, requiring the user to repeat the process each time he or she revisits the site. This increases the chances of the user downloading malware surreptitiously. This mandated process is also a problem for frustrated users, whose interaction with these sites is constantly being interrupted by notifications of required downloads. He or she must then agree to the download while simultaneously acknowledging the risks of doing so. The idea behind this process is that allowing a user to control downloads to his or her system will provide greater scrutiny of what is being downloaded, and thus help prevent the infiltration of malware. How-

23. Park Hun Myoung, "45th Hawaii International Conference on System Sciences: (HICSS 2012) Maui, Hawaii, January 4-7, 2012," *Proceedings of the Web Accessibility Crisis of Korea's Electronic Government*, "Fatal Consequences of the Digital Signature Law," New York: IEEE, 2012, 2319-28.

ever, considering that the website cannot be accessed properly without downloading the plug-in, a user's only choices are to either download the program or to not use the site. It is the contention of the author that most users choose the former on a consistent basis. Furthermore, their repeated acceptance of these downloads desensitizes them to the dangers of such actions, and increases the number of system incursions.

In a 2014 study on South Korean internet users' on-line behavior, the author of this paper conducted a survey on the response of South Koreans to security plug-ins, specifically ActiveX.[24] The results were telling. 17.32% of participants responded that they automatically downloaded all security plug-ins whenever instructed to do so, and 37.02% responded that they usually download the ActiveX -delivered plug-in. Only 12.6% said that they seldom download plug-ins, with only 1.57% responding that they never download such plugins (Table 1). When asked if their home computer had been rendered inoperable due to malware, 32.2% responded that their system crashed one time as a result of malware, 63.5% encountered this situation multiple times, while only 4.3% reported that they had never been hacked in that manner (Table 2).

Table 1. Reaction to Warning Prompt

Action	%
Always "allow" to view the website?	17.32
Usually "allow" to view the website?	37.02
Sometimes "allow" to view the website?	29.92
Seldom "allow" to view the website?	12.6
Never "allow" to view the website?	1.57
Investigate further	1.57

24. J. Gustave Swanda, "The Dilemma of Software Uniformity and Cybersecurity in South Korea" (Ph.D. Dissertation, Pukyong National University, 2016), pp. 105-107.

Table 2. Compromised CPU or Mobile Device (Home)

Has your personal mobile device or PC been rendered inoperable by malware? If so, how many times?	%
Yes, only once.	32.2
Yes, more than once.	63.5
No, my home computing device has never stopped working due to malware	4.3

In 2005, the Ministry of Public Administration and Security (MOPAS) had jurisdiction over the NPKI, and amended the ID requirement to apply only to the websites of government institutions and websites that are involved in financial transactions or information.[25] Later, amendments also required that systems abandon ActiveX by 2017.[26] Despite these revisions, there are still many educational institution, government, banking, and e-commerce websites that fall under the original provision, and thus are required to employ ActiveX or similar plugins which have the same problems and vulnerabilities.

Psychological Constraints

The way citizens perceive their government's role in cyberspace varies greatly from state to state. Culture, history, and demographics are all determinant factors of a nation's psychology on issues such as privacy,

25. Hun Myoung Park and Hanjun Park, "Diffusing the Information Technology Education in the Korean Undergraduate Public Affairs and Administration Programs: Driving Forces and Challenging Issues," *Journal of Public Affairs Education* 12, no. 4 (2006).
26. In March of 2015, the Federal Services Commission and the Ministry of Science, ICT, and Future Planning repealed the ActiveX requirement for only transaction verification. However, financial institutions are still required to have a security plugin to verify the identity of online consumers. In addition, the MSIP and FSC announced a new, updated version of *ActiveX*. Sung-won Yoon, "*ActiveX* to be Phased Out in March," *The Korea Times*, January 14, 2015, http://m.koreatimes.co.kr/phone/news/view.jsp?req_newsidx=171687 (accessed July 5, 2015).

freedom of information, intellectual property, libel, and trust in the government. Cyber borders may be psychologically acceptable in one society, but not in another. These sui generis elements of the national psyche may also impede the transition to a Westphalian internet.

In China for example, the government has met very little resistance to its restrictive internet policies. Beginning in the mid 1990's, successive regulations have increasingly limited what Chinese citizens can say or access online. This led to the creation of Section Five of the Computer Information Network and Internet Security, Protection, and Management Regulations approved by the State Council on December 11, 1997 which states:

> "No unit or individual may use the Internet to create, replicate, retrieve, or transmit the following kinds of information:
>
> 1. Inciting to resist or breaking the Constitution or laws or the implementation of administrative regulations;
> 2. Inciting to overthrow the government or the socialist system;
> 3. Inciting division of the country, harming national unification;
> 4. Inciting hatred or discrimination among nationalities or harming the unity of the nationalities;
> 5. Making falsehoods or distorting the truth, spreading rumors, destroying the order of society;
> 6. Promoting feudal superstitions, sexually suggestive material, gambling, violence, murder;
> 7. Terrorism or inciting others to criminal activity; openly insulting other people or distorting the truth to slander people;
> 8. Injuring the reputation of state organizations;
> 9. Other activities against the Constitution, laws or administrative regulations."[27]

In addition to censorship of government criticism online, many commercial and social networking sites such as Google and Facebook have been banned and replaced by their domestic counterparts. There are as

27. Jason P. Abbott, *The Political Economy of the Internet in Asia and the Pacific Digital Divides, Economic Competitiveness, and Security Challenges* (New York: Praeger, 2004), p. 56.

many as 18,000 websites that are blocked by the Chinese government.[28] Penalties for violating these rules or using virtual private networks to circumvent policy can be harsh. But despite the threat of imprisonment, there is still a subdued counterreaction to government actions often through satire and sarcasm. "Chinese websites made subtle grievances against the state's censorship by sarcastically calling the date of June 4th (the anniversary of the 1989 Tiananmen Square massacre) as "Chinese Internet Maintenance Day."[29] Perhaps this type of subtle acknowledgement of censorship while still complying with government policy would be psychologically manageable in China, but would most likely be an atypical reaction to a government restricting the internet in other countries.

There are also those nations that have sought to control the flow of certain sensitive foreign and domestic information only to find their efforts undermined by a citizenry not willing to conform to state standards. The best example of this is the Arab Spring. Despite the ban on social networking and outside media sites, citizens of Tunisia, Egypt, Libya, Yemen, Syria, and Bahrain were all able to utilize banned sites to organize protest movements, disseminate censored information, and eventually bring down many of those regimes.

The South Korean Government has also seen a surprising reaction from its self-proclaimed "netizens" towards restrictive cyber policy. Such reactions are often unexpected in a country renowned for conformity. In 2008, policymakers felt Korean bloggers were acting irresponsibly by circulating rumors over the dangers of contracting mad cow disease from American beef imports and posting malicious comments about celebrities under pseudonyms. Public fervor ignited when popular actress Choi Jin-sil committed suicide. There was widespread speculation that negative comments posted about her on the internet led to her suicide, and demands were made on legislators to prevent

28. Johnathan Zittrain and Benjamin Edelmin, "Empirical Analysis of Internet Filtering in China," December 30, 2006, https://cyber.harvard.edu/filtering/china/ (accessed March 12, 2016).
29. Bobby Johnson, "Chinese Websites Mark Tiananmen Square Anniversary with Veiled Protest," *The Guardian*, June 4, 2009.

users from posting comments anonymously. In 2008, the so-called "real-name internet" law was passed, which required people to use their real name, verified by their national identification number when posting comments on the internet.[30] At first, internet users tolerated the restrictions on their freedom of expression. But as cases of retribution by netizens against individuals who posted negative comments on message boards grew, and after a system hack that led to a breach of millions of South Korean identification numbers, public opinion on the real-name law soured. The massive protests against the law and public outcry from mostly younger Koreans sparked a movement that eventually spilled over into the mainstream. Finally in 2012, the constitutional court overturned the law finding that it "is unconstitutional, and such provisions are in violation of the principle of less restrictive alternative expression and freedom of speech of both users as well as ISP's in the cyberspace, and the self-dissemination of personal information."[31] Part of controlling national cyber borders would be to mitigate the negative public perception that accompany such measures. However, a survey done by the Federation of Korean Industries (FKI) showed that 78.6% of users wanted to get rid of ActiveX, and 88% experienced some sort of difficulties because of ActiveX.[32] As was the case with South Korea, such unforeseen perceptions are often uncontrollable and difficult to predict.

The crux of the problem was that Microsoft Windows is the only platform that supports ActiveX. This forced all online businesses and their users to exclusively use Microsoft Windows. Consumers were also forced to use Internet Explorer as it alone supported ActiveX. This resulted in website developers, along with banking and shopping sites, optimizing all websites for Internet Explorer. It became the South Korean industry standard in web development, which has given

30. Article 44-5 (Authentication of On-line Bulletin Board User) of the Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. (정보통신망 이용촉진 및 정보보호 등에 관한 법률).
31. Constitutional Court Decision 2010Hun-Ma47 decided on August 23, 2012.
32. "South Koreans Overwhelmingly Approve of Scrapping ActiveX: Poll," *Yonhap News Agency*, March 23, 2014.

Microsoft a near monopoly on Korean operating systems and web browsers for over a decade.[33]

This policy seemed prudent at the time, and initially limited the traffic from foreign users and potential threats. The program became obsolete around 2005, yet the policy remained long after that. Malicious codes can easily be embedded to circumvent ActiveX making the program virtually useless. It seems the Windows/ActiveX platform, although cutting-edge in 1998, left systems near defenseless by 2013. Turn of the twenty-first security assets like ActiveX, were liabilities when it came to the hacking techniques of 2013. They proved to not be a very effective shield against today's viruses and malware, or against the ingenuity of today's hackers.

However, political discord, national security concerns, and the technology market turned such levels of national control into political liabilities, and forced the South Korean government to effect change in this area. In 2011, after pressure from makers of alternative technologies such as smart phones forced the government to rethink their 10 year-old cybersecurity strategy, the government created a bylaw calling for the support of at least three different web browsers on government websites. Even if varying the browser support for government websites could change the now embedded on-line behavior of developers and users, implementing change is very difficult. In order for websites to stop using ActiveX plug-ins, a government appraisal committee must evaluate the new technology to ensure it has the same level of security. However, the committee did not approve any alternative websites since its inception for over four years.[34] So by moving farther away from the rest of world, the South Korea government actually put its country's cyber infrastructure closer to harm's way.

---

33. Glen Moody, "South Korea Still Paying the Price for Embracing Internet Explorer a Decade Ago," *Tech Dirt*, May 9, 2012, https://www.techdirt.com/articles/20120507/12295718818/south-korea-still-paying-price-embracing-internet-explorer-decade-ago (accessed June 29, 2016).
34. Moody, "South Korea Still Paying the Price for Embracing Internet Explorer a Decade Ago," 2012.

Stuxnet

The Stuxnet virus is an exemplar of a cyber threat with catastrophic, real-world consequences, which is a key element in Demchak and Dombrowski's model. It not only shifts policy focus towards a radically new method of cyber defense, but it also serves as the fulcrum by which public opinion is swayed towards cyber borders. However, is that a fair representation of Stuxnet's salience? It is not entirely certain whether or not Stuxnet conforms to Demchak and Dombrowski's characterization as a catalyst for a new internet paradigm. To ascertain this, the nature of the malicious code must be analyzed as well as its relation to cyber-threat strategy.

Stuxnet was a large, densely coded computer virus designed specifically to attack the synchronization mechanisms of the uranium centrifuges at the Iranian nuclear facility. The virus replicated itself and spread throughout the targeted system by utilizing a "zero-day" exploit, a very rare and dangerous method of attack.[35] A zero-day exploit takes advantage of specific vulnerabilities in the software of the host at the time of the incursion. With no defensive obstacles to confront, nor any possibility of detection, the exploit spreads very rapidly making containment extremely difficult if not impossible. The first Stuxnet zero-day exploit spread itself to other sections of the centrifuge's systems by infecting the USB sticks of users. This exploit was necessary, as the different sections of the centrifuge system, like that of many highly-secured systems with catastrophic potential, were not connected to each other nor to cyberspace. Throughout each section, Stuxnet scanned the system in search of its target: the industrial

35. Due to the difficulty of engineering a new virus that operates in a completely different manner than any other malware, and thereby avoiding both detection within the system and in the computer virus security zeitgeist, zero day malware is very rare. Less than one in 1,000,000 malicious code uncovered are zero days. They require the creator to meticulously test every part and line of a software's code; a process that can take years (Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," 2011).

control system used to program controllers that drive motors, valves, and switches in industrial facilities. In order to execute new commands to these industrial control systems on a Windows platform, the virus must have an electronic certificate specific to that piece of hardware, the contents of which are known only to a few at Microsoft, the manufacturer of the industrial equipment, and the end user. Forensic examination of the virus revealed that it used a valid, signed certificate stolen from Realtek's hardware manufacturing facilities in Taiwan. This is no easy feat, leading experts to believe that the creators of the virus had access to an extensive intelligence network.[36]

Further investigation showed that Stuxnet had not one but three zero-day exploits in addition to 500 kilobytes of other malware coding, a very large program compared to the average 10 to 15 kilobyte-sized virus. Workers at the Iranian facility used Stuxnet-infected USB sticks in both the centrifuge's system and outside the system on work and personal computers. This caused an enormous amount of collateral damage, which is how Stuxnet was finally discovered.[37] Each time Stuxnet replicated itself it would contact one of two domains (websites) in either Malaysia or Denmark. After securing the cooperation of the domains' DNS providers, investigators discovered that Stuxnet had infected over 100,000 machines, a majority of which were in Iran. Through trial and error, Stuxnet was attempting to upload itself to the USB of someone who worked at the nuclear facility, where it could download itself and eventually reach its intended target.[38]

The specificity of this virus' functions is worth noting, as it makes applying Stuxnet to another system with a different goal virtually

36. Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, July 11, 2011, https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/ (accessed June 13, 2016).
37. Michael Joseph Gross, "A Declaration of Cyberwar," *Vanity Fair*, March 2011, http://www.vanityfair.com/news/2011/03/stuxnet-201104 (accessed October 20, 2015).
38. Ralph Langer, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," *The Langer Group*, November, 2013, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf (accessed July 6, 2016).

impossible. Today the usefulness of the Stuxnet virus is in essence dead. It had one specific goal, and that goal was achieved. Although unintended residual effects from Stuxnet were felt by systems in cyberspace for some time afterwards, the coded commands would only have its intended effect on the Iranian centrifuge. Once the virus was discovered and deconstructed, cybersecurity firms were able to tag its specific characteristics, allowing most security programs and firewalls to detect and block the virus. The entirety of Stuxnet's code has since been open sourced, however the fear that an international actor could employ the same or similar techniques found in Stuxnet remains.

While Demchack and Dombrowski's claim of Stuxnet causing a panic among states and shifting emphasis towards borders appears to be correct, it would be inaccurate to claim that such trepidation is due entirely to Stuxnet. The fear of a cyber doomsday weapon existed long before Stuxnet's creation. In 1996, then CIA director John Deutch, told a Daily News interviewer that hackers "could launch "electronic Pearl Harbor" cyberattacks on vital U.S. information systems." Shortly thereafter at a U.S. Senate Governmental Affairs Permanent Subcommittee on Investigations hearing, Deputy Attorney General Jaimie Gorelick reiterated Deutch's fears by telling subcommittee members, "we will have a cyber-equivalent of Pearl Harbor at some point, and we do not want to wait for that wake-up call."[39] These statements by high-level government officials started the ball rolling towards domestic cyberdefense policy, as anti-terrorist efforts in the U.S., China and Europe slowly began shifting focus to include cyber threats, the idea being that a large scale cyberattack against a nation's critical infrastructure could be as devastating as conventional terrorism or acts of war. Even after the terrorist attacks on Washington and New York on September 11, 2001, when national security policy was reevaluated, many inside and outside the government believed the next big attack would happen in cyberspace.

---

39. Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," 2011.

Furthermore, it can be inferred from the Stuxnet experience that cyber borders would be ineffective against a zero-day threat like Stuxnet. The virus showed that connectivity is not necessary to infiltrate secure, closed systems. After all, the virus' success was dependent upon the intelligence gathered for its creation and implementation. It is not unrealistic to assume that the distribution of such a cyber weapon could just as easily be distributed in a national cyber domain, given the intelligence and resources necessary for the attack.

Economic Effects

Another aspect that is overlooked in the Westphalian model is the economic effect that national divisions in cyberspace may have. Such effects were evident in the development of South Korean early e-commerce policies related to the Digital Signature Act. The government's early cyber policy tried to stop cyber fraud by regulating the architecture of doing business over the internet. This was a part of the rationale behind the mandatory identification number verification policy. Requiring patrons to download the identification plug-in (ActiveX), enter a national ID number, and other such verifications made it almost impossible for South Korean companies to serve customers outside of Korea. Meanwhile, Korean online shoppers increasingly frequented foreign e-commerce sites, due in part to the previously mentioned compatibility issues between the plug-in and non-Microsoft operating and browsing software. This led to an erosion of online business across the board in South Korea, a development lamented by South Korean companies. In March of 2014, the FKI lobbied President Park Geun Hye and the South Korean legislature to repeal the ActiveX and ID entry policy. Data from the Korea Institute for Industrial Economics and Trade showed that despite having greater connectivity and superior internet infrastructure than most of its foreign counterparts, South Korea's on-line shopping sector was only 2.69 billion USD or .24% of its GDP, compared to 1.24% in the

U.S. and 1.68% in China.[40]

Although the president promised to replace ActiveX with a less restrictive and more interactive plan, ActiveX or similar plugins remain in place for verifying financial transactions. In order for cyber borders to be viable, they must allow the free flow of commerce over the internet. A centrally controlled national cyberspace could very well experience the same problems as South Korea, or worse. This issue would present a problem that policymakers would have to address first and foremost when devising strategies to exert greater sovereignty over the internet.

Conclusion

Demchack and Dombrowski have presented some sound arguments for the "transformation from frontier to substrate across cyberspace," and many of their postulates, are in fact, indisputable. Governments are indeed seeking to define national cyber boundaries, and to have greater control over the electronic data within their borders. If technology, the politic and, most importantly, their constituencies would allow it, an international cyber Westphalian system could become an inevitability. However as South Korean forays into these boundaries have shown, the limitations of technology, the inefficiency of the political process, and the diversity of the national psyche mean that such a system could not feasibly be realized in the form Demchack, Dombrowski, and others have imagined. If and when liberal democracies attempt to implement such policies, the negative effects to both the economic and systemic base of national cyberspace may be enough to force most nations to seek alternative strategies. The establishment of shared international norms for cyberspace and international agreements on cybersecurity are not necessarily accompanied by cyber

40. Sam Reynolds, "Korea's ActiveX Problem," *VR-Zone*, March 25, 2014, http://vr-zone.com/articles/koreas-activex-problem/74622.html (accessed March 14, 2016).

borders.

In the case of South Korea, there has been a consistent push towards centralizing control of national cyberspace. Despite a majority of users regularly following the government-mandated protocols on a regular basis (54.34%), an overwhelming amount (95.7%) have had their systems compromised at least once.[41] These numbers do not support the idea that a strong, centralized government-run cyberspace is any more secure than a PKI that operates outside of government control. Although the government has repealed its mandate of ActiveX, it has simply replaced it with new protocols for downloading plug-ins. This may bring similar problems, and possibly more impediments to the free flow of information and commerce domestically and internationally. There is anecdotal argument to be made against centralization of the internet as well. Throughout the government's attempts to secure its cyber infrastructure over the past decade, the country has been plagued with many successful, high-profile cyberattacks on industry and the government. This may be a sign that the government needs a new tactic. In order to avoid the economic and logistic pitfalls of a tightly sanctioned internet, policy makers should consider following the examples of other countries, and leave the responsibility for commercial and personal cybersecurity up to trusted browsers and the individuals themselves.

Bibliography

Abbott, Jason P. *The Political Economy of the Internet in Asia and the Pacific Digital Divides, Economic Competitiveness, and Security Challenges*. New York: Praeger, 2004.

Bennett, Larry D. "Cryptographic Services — A Brief Overview." *SANS Institute InfoSec Reading Room*, October 10, 2001. https://www.sans.org/reading-room/whitepapers/vpns/cryptographic-services-overview-749.

41. Swanda, "The Dilemma of Software Uniformity and Cybersecurity in South Korea," pp. 105-107.

Cardenas, Edgar D. "MAC Spoofing: An Introduction." *GIAC Security Essentials Certification (GSEC)*, August 23, 2003. https://www.giac.org/paper/gsec/3199/mac-spoofing-an-introduction/105315.

Cisco, Systems. "Defending Cyber Borders: Beyond the Virtual Maginot Line." 1105 Media and Cisco GovEduTV Interactive video cast, October 25, 2012. http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/fedbiz121212maginot.pdf.

Clark, Richard A. and Knake Robert K. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: Harper Collins, 2010.

Delfs, Hans and Knebl Helmut. "Symmetric-key Encryption." *Introduction to Cryptography: Principles and Applications*. Berlin, Heidelberg, New York: Springer, 2007.

Demchak, Chris and Dombrowski Peter. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* 5, no. 6 (2011): 32, 34-35.

Hare, Forrest. "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?" *School of Public Policy, George Mason University Cryptology and Information Security Series Volume 3: The Virtual Battlefield: Perspectives on Cyber Warfare* (2011): 88-105, DOI: 10.3233/978-1-60750-060-5-88.

Heal, G. and Kunruther H. "Self-protection and Insurance with Interdependencies." *Journal of Risk and Uncertainty* 36, no. 3 (2008): 103-123.

Himanshu, Arora. "TCP/IP Protocol Fundamentals Explained." *The Geek Stuff*, November 2, 2011.

Holcomb, Lee and Shrewsbury June. "Securing Our Cyber Borders." *Innovation* 9, no. 1 (February/March 2011). http://www.innovation-america.org/securing-our-cyber-borders.

Johnson, Bobby. "Chinese Websites Mark Tiananmen Square Anniversary with Veiled Protest." *The Guardian*, June 4, 2009.

Kim, Keechang. "Recent Changes in the Regulatory Landscape for E-Commerce in South Korea." *The Asian Business Lawyer* 16 (Fall 2015): 87-103. file:///C:/Users/user/Downloads/04.Keechang Kim_article (3).pdf.

Korea Times. "For World's Most Wired Country, Breaking Internet Monopoly is Hard." *Korea Times*, April 16, 2012. http://www.koreatimes.co.kr/www/news/biz/2012/04/123_109059.html.

Langer, Ralph. "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve." *The Langer Group*, November, 2013. http://www.langner.com/en/wpcontent/uploads/2013/11/To-kill-a-centrifuge.pdf.

Maher, Katherine. "Cybersecurity: 'The New Westphalian Web'." *Truman National*

Security Project Doctrine Blog, February 25, 2013. http://trumanproject.org/doctrine-blog/cybersecurity-the-new-westphalian-web/.

Menn, Joseph. "U.S. Tried Stuxnet-style Campaign against North Korea but Failed." *Reuters*, May 29, 2015. http://www.reuters.com/article/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529.

Moody, Glen. "South Korea Still Paying the Price for Embracing Internet Explorer a Decade Ago." *Tech Dirt*, May 9, 2012. https://www.techdirt.com/articles/20120507/12295718818/south-korea-still-paying-price-embracing-internet-explorer-decade-ago.

Park, Hun Myoung. "45th Hawaii International Conference on System Sciences: (HICSS 2012) Maui, Hawaii, 4-7 January 2012." *Proceedings of the Web Accessibility Crisis of Korea's Electronic Government*: "Fatal Consequences of the Digital Signature Law." New York: IEEE, 2012. 2319-28.

Park, Hun Myoung and Park, Hanjun. "Diffusing the Information Technology Education in the Korean Undergraduate Public Affairs and Administration Programs: Driving Forces and Challenging Issues." *Journal of Public Affairs Education* 12, no. 4 (2006).

Reynolds, Sam. "Korea's ActiveX Problem." *VR-Zone*, March 25, 2014. http://vr-zone.com/articles/koreas-activex-problem/74622.html.

South Korea, Ministry of National Defense. *Defense White Paper 2008*. Seoul 2008.

Swaine, Michael D. "Chinese Views on Cybersecurity in Foreign Relations." *China Leadership Monitor*, September 20, 2013.

Swanda, Gus. "The Dilemma of Software Uniformity and Cybersecurity in South Korea." Ph.D. Dissertation, Pukyong National University, 2016.

Yonhap News Agency. "South Koreans Overwhelmingly Approve of scrapping ActiveX: Poll," Yonhap News Agency, March 23, 2014.

Yoon, Sung-won. "ActiveX to be Phased Out in March." *The Korea Times*, January 14, 2015. http://m.koreatimes.co.kr/phone/news/view.jsp?req_newsidx=171687.

Zetter, Kim. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." *Wired*, July 11, 2011. https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

_____. "Stuxnet Attack on Iran Was Illegal 'Act of Force'." *Wired*, March 25, 2013. https://www.wired.com/2013/03/stuxnet-act-of-force/.

Zittrain, Johnathan and Edelmin Benjamin. "Empirical Analysis of Internet filtering in China." December 30, 2006. https://cyber.harvard.edu/filtering/china/.