**Solving Intrinsic Dilemmas in Cybersecurity Policymaking with the PACE Model: Principles and Applications**

**Elif Sercen Nurcan[[1]](#footnote-1)**

The current cybersecurity landscape consists of constantly increasing low intensity incidents with spikes of high intensity engagements. Unlike the traditional understanding of security, the provision of cybersecurity is an ongoing product of arrangements between the state, private sector, and citizens. In this system of shared responsibility, the state’s role is policymaking which entails intrinsic dilemmas. Key dilemmas in cybersecurity policymaking are formulated in the first section of this study alongside root causes. In the second section, a solution framework is given as the ‘public attention-constant escalation model’ (PACE Model) which is built upon pairing of quantitative search query data and incident timeline information. Via the pairing, the model identifies optimal windows of short-term reactionary policies alongside long-term proactive policies. In order to test the durability of the model’s proposals for dilemma solution, Japan’s cybersecurity policies for Tokyo 2020 Olympics are taken under consideration in the last section. Per the results, overcoming intrinsic dilemmas in cybersecurity policymaking is found to benefit from systematic identification of optimal policy windows.

Keywords: Cybersecurity, policymaking, cybersecurity policies, policy framework

**Introduction**

Cybersecurity presents a new policy area for states. It has evolved national security to the point of involving technology in unprecedented ways. For example, IoT (Internet of Things) devices which can access Internet have been used to launch massive attacks by the billions, leaving states to scramble for countermeasures. The sharp division between the security responsibility of the state and its subjects is also blurred by dynamic interactions, conflict, and contestation (Deibert and Rohozinski 2012, 31).

Technical works on cybersecurity issues are numerous and far removed from any of the policymaking aspects (Cavelty and Egloff, 2019, 41). In social science literature, studies on cybersecurity often feature analyses of military and international relations (Barkin, 2018; Taipale, 2010). There are also works on cybersecurity policy which focus on the developments in policymaking history (Soesanto, 2020; Orden, 2019). However, there is a lack of social science studies which look at the process of cybersecurity policymaking. This paper takes on the task and focuses on key dilemmas in cybersecurity policymaking. One further step is taken to provide a framework for the solution of the identified dilemmas in the form of a model called PACE Model (Public Attention-Constant Engagement Model).

This study is divided into three sections. In the first section, the current cybersecurity landscape and cybersecurity policy issues are summarized. In the second section, cybersecurity policymaking process is analyzed in terms of dominant issues in order to identify the fundamental dilemmas. The constituents of PACE model are also given in this section; a modified understanding of the Overton Window is adapted for building the concept of policy time scales while the constant engagement principle of the model is taken from the cybersecurity policy components. In the last section, a brief case study is carried out for testing the durability of the PACE model. The findings are built, based on, and supported by search query data from Google Trends, author’s observation of online events, and cybersecurity-related data collected by verified research firms. Overall, the results are new to the political science field as principal dilemmas in cybersecurity policymaking are named and a model is offered to identify the policy windows based on a perspective that combines the factors of public attention and constant engagement.

**1. The current situation of cybersecurity landscape and policymaking**

One of the defining characteristics of the current cybersecurity landscape is the double-edged sword of cyber tools. The widespread internet penetration into the society has caused a paradox where the citizens are more productive and prosperous at the cost of being vulnerable (Manjikian, 2021, 21); the state enjoying newly found digital sovereignty at the cost of being dependent on cyberspace (Konen, 2021). Vulnerability stems from threats which refer to malicious cyberattacks that seeks to unlawfully access data, disrupt digital operations or damage information by actors “… including corporate spies, hacktivists, terrorist groups, hostile nation states, criminal organizations, lone hackers, and disgruntled employees” (University of North Dakota, 2022).

Another defining characteristic is the enormous volume of data on the global cyberspace. Relatedly, the current cybersecurity landscape is marked with a constantly growing number of cyberattacks. For example, the use of malware has increased by 358% through 2020, and ransomware usage increased by 435% compared to the previous year, according to a study by Deep Instinct. Continuous increase in online malicious activities is the reality of today; July 2020 alone saw a 653% increase in malicious activity compared to the same month in 2019 (Help Net Security, 2021).

Figure 1: Increasing global malware infection growth rate, 2009-2018

Source: PurpleSec, 2022.

It is not possible to capture the entirety of the online malicious activities data due to the size and the reported incidents’ making up only a very small portion of all attacks. This ever-increasing number of cybersecurity incidents is coupled by the addition of new issues and threats. Users are facing issues in cyber governance such as net neutrality and user issues of malvertising, impersonation, cybercrime, geolocation, and privacy violations. Cybersecurity threats have evolved to include sophisticated tools such as ransomware, emotet, denial-of-service, man-in-the-middle, phishing, SQL injections, etc. (University of North Dakota, 2022).

Alongside the increase in cyberattacks, public interest in cybersecurity has also risen. To illustrate, Google Trends can be utilized as a method of measuring public interest. Internet user search queries on Google show “interest over time”, with the numbers representing search interest relative to the highest point on the chart for the given region and time; a value of 100 being the peak popularity for the term and a score of 0 meaning there was not enough data for the term (Google 2022). Peaks and troughs occur as public attention wanes from the topic of cybersecurity at times and becomes renewed with memorable events.

Figure 2: Historic trend of Google searches for “cybersecurity”, January 2016-March 2022

Source: Google Trends, 2022.

In the background of these constantly shifting trends in cyberattack volumes and public attention, states have to constantly produce policies to face the onslaught. However, the policymaking process itself is facing issues, as discussed in the next section.

**2. Cybersecurity policy issues and policymaking dilemmas**

**2.1. The current cybersecurity policy issues**

Rapid technological change throughout the internet era has led to the legislation and the ability to regulate technology lagging behind the technology itself. This situation is exacerbated by the addition of other issues which can be traced to the results of orthodox practices in policymaking clashing with the new technological aspects.

**1. Sovereignty issue**: The new non-traditional cybersecurity issues challenge the state’s monopoly over legitimate violence over a certain territory. Actors active in cyberspace who may pose threats are not necessarily limited in geography or predetermined notions of capability. Groups of threat actors may lay scattered all over the globe, possessing seemingly small attack capabilities which may in fact become scalable with new technology breakthroughs. In addition, cyberhackers, cyber activists, cybercriminals, etc. operate with different motivations and react differently to security provision measures. The combination of these factors put stress on the state. Different states with different governance models and alternating understanding of security have naturally responded to this situation in ways reflective of their principles. However, the common point uniting states is the threat on their implementation of nationwide policies with executive privileges.

Even though nations are legally equal in the Westphalian sense of sovereignty, they are technologically and economically disparate (Shackelford, 2020, 5). These disparities open the way for unorthodox operations. For example, evidence of election interference by foreign states or their proxies has become a regular feature of national elections in democracies and is likely to get worse. Previously unimaginable operations such as closed social media platforms, algorithms that prioritize extreme views and inflammatory disinformation, misinformation, and malware interfere with normal functions of governance. Indeed, false information is not a violation of sovereignty but disrupting computer programs which alter voting tabulations are (Velde, 2021, 164-165). Cyberspace-enabled influence operations can be and are conducted using existing institutions to shape politics.

**2. “War or no war” issue**: Cyber peace is not the absence of attacks or exploitations. In addition, there is no more than a vague consensus as to what constitutes an act of cyberwar. For example, the US National Academy of Sciences defines cyberattacks as deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks where probes are not equal to attacks. According to the Tallinn Manual (2nd edition, 415), “A cyberattack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.” Cyberattacks can be simultaneously acts of war, terrorism, political/military/corporate espionage, or crime. Cyberattacks by any name will continue to evolve, challenging laws, norms, markets, architectures, and policies to keep up (Shackelford, 2020, 23). One common point seems to be that if perpetrators of cyberattacks are states, governments, militaries, then the act is generally considered cyberwar while if non-state actors commit the act, then it is hard to say it is war (Tsuchiya, 2016, 181).

**3. Capacity and responsibility issue:** The real final payoff of cybersecurity is tied whether the general population of Internet users in a nation actually experience the benefits of a more secure cyber environment, an outcome that is difficult to reliably measure (Dutton, Creese, Shillair, Bada, 2019, Cybersecurity Capacity: Does It Matter?, 302). National cybersecurity capacity building involves the development of managerial, technical, social, legal, policy, and regulatory initiatives by a growing ecology of actors to enhance the resilience of nations to cybersecurity breaches, cybercrime, and terrorism (280). As an enabling environment, cybersecurity capacity ranges from policy and strategy to sociocultural attitudes, knowledge and skills, regulations, law enforcement, and technical standards and capabilities.

In this understanding of responsibilities, an analogy can be drawn between cybersecurity and fire control. There are fire departments operating on public funds to respond to fires when necessary. These fire departments are responsible for putting out large fires and do damage control and rescue. But by law, people and organizations are required to have fire extinguishers in their homes and offices, in addition to having training to use them. Each individual and organization has responsibility to put out fires around them and rescue others. This is very similar to provision of cybersecurity where the state has the largest responsibility to protect and to do damage control, however, individuals and organizations have responsibility to do the same.

**4. Public-private sector partnership issue:** This issue is particularly related to the capacity and responsibility issue above. The private sector is increasingly aware of the importance of cybersecurity (Yu, 2022). Hundreds of IT executives around the world point out at the challenges of accelerating digital applications while constantly ramping up the organization’s digital transformation. It’s now imperative for organizations to establish a continuous and repeatable cyber risk and compliance management program (GigaSpaces Webinar 2022). With constant technological improvements and increasing digital transformation to the cloud, many organizations’ threat landscapes have complexified with new vulnerabilities and a larger attack surface.

According to the logic of the market, a firm will invest in cybersecurity at a level where the marginal private return from that investment equals the marginal private cost. However, the society, as represented by the state, would like this firm to increase its investment in cybersecurity to a level where the investment level corresponds to marginal social benefits. For a firm to agree to do this, its marginal private cost must decrease. If the government could provide support to lower marginal private costs to the point where the new marginal private cost equals marginal private return, then this socially desirable level of investment will be undertaken by the firm” (Gallaher, Link, Rowe, 2008, 131). The associated threat of litigation from being out of compliance or causing damage to a second party is another way to make private organizations come under a public-private partnership. As of currently, this issue of forging partnerships remain unresolved.

**2.2. Dilemmas in cybersecurity policymaking**

Moving on from the cybersecurity policy issues discussed previously, there are common points in cybersecurity policymaking which are entrenched and not easily overcome. These common points are dilemmas. The cause of all dilemmas stem from the fact that cybersecurity policymaking incorporates traditional security perspectives, goals, and conflicts despite its novel status. Also, the increased scalability and agglutinative nature of cybersecurity policy areas constitute another cause. Generally, there are three main dilemmas in cybersecurity policymaking identifiable. These dilemmas present the most vital challenges policymakers must face when making decisions.

The first dilemma in cybersecurity policymaking is the “dilemma of securitization”. The importance of cybersecurity can't be overstated. However, if everything in cybersecurity is taken as essential and “securitized” via speech and other actions, then nothing can take precedence. The root cause of this dilemma is as follows. In cybersecurity, limited attention and human resources cannot be dispersed across all areas. Policy may not achieve anything unless there is a clear prioritization of cybersecurity policy goals. To tackle this challenge, states can look into spending resources for building state-action models in cybersecurity that reflect their traditional security priorities and cybersecurity capabilities. Models can assist in solving the securitization challenge if they are presented properly and consistently across all shareholders.

The second dilemma is the “red sequoia dilemma”. As red sequoias are extremely tall and thus, eye catching trees, there are certain policy targets and areas which receive more attention due to their being more established. This is not to dispute the fact that some of these policy targets and areas are vital; this dilemma is born from the overlooking the previously unexplored policies and overfocusing on the previous sets. Without conscious effort to branch out policies, policymakers risk not meeting cybersecurity needs which itself can prove to be damaging.

The third dilemma is the “mutual assured destruction (MAD) dilemma”. Due to the aforementioned issue of attribution being one of the most difficult issues to resolve in cybersecurity (Tsuchiya, 2016, 180) and constantly increasing volumes of cyberattacks, it is not possible to determine what constitutes a first strike and who the responsible party is in a timely manner. The original MAD doctrine also stipulates equal striking capabilities between the opposing parties, a factor rare in the asymmetrical world of cybersecurity capabilities. However, policymaking process has to incorporate the possibility of a MAD situation where parties to the conflict may inflict system destructive level of harm. To prepare, cybersecurity policies should be adjusted as tools to help a state compete and survive in ever going conflicts. In other words, there have to be different policies running on varying timescales in operation at the same time.

These dilemmas cannot be resolved easily as the mismatch between the policymaker, technical, and defense perspectives are deep. The language employed by each policy actor also differs. The minute priorities of each side are also different despite the common goal of achieving security. To prevent breakdown of chain of command during acute crises, a well communicated model of cybersecurity is needed. Such a model would have to provide the systematic communication required for the dilemma of securitization, multiplicity of policy targets for the red sequoia dilemma, and the time scale for the MAD dilemma. The PACE model is configured to meet these requirements as explained in the next section.

**3. The PACE Model**

**3.1. Building the PACE Model**

According to Fadi Chehade, producing coherent cybersecurity and digital norms is difficult due to the widegap in understanding nature of designing and implementing such norms- gap across all sectors, public, private, and civic. This gap is exacerbated by internet’s transnational nature, its speed of borderless reach, relentless digital innovations it enables, and emergence of powerful digital platforms operating without borders. Stakeholders have to evolve past 20th century governance mechanisms for modern, agile, and legitimate governance mechanisms to produce norms necessary for economic growth and innovation, limited weaponization of critical infrastructures (Shackelford, 2020, xiv-xv). It is important to adequately take general countermeasures and not only individual ones for various incidents during times of peace in addition to knowing incident types and cyberattack methods for avoiding attacks and not becoming a direct target (Masujima, 2020, 146). By answering these demands, the PACE Model can be used as a dilemma solution framework in cybersecurity policymaking. The model does this by identifying the optimal policy adaptation windows based on an understanding of different time scales of policies and intensities.

**3.2. Constant engagement and cybersecurity policymaking**

Cybersecurity policy carries importance in relation to both strategy and operations, its relevance to a very diverse set of stakeholders and decisionmakers. But it also creates controversies and debates. Policy goals forged by national security concerns, domestic politics, and psychological needs give shape to complicated cybersecurity policies. Some of the guidelines are practical, but most are conceptual. In real life, policy problems appear as an entanglement of details such as personalities, interest groups, rhetorical demands, budget figures, legal rules interpretations, bureaucratic routines, citizen attitudes, and so on (Bardach, 2012, xvii).

Table 1: Components of public cybersecurity policy

|  |  |
| --- | --- |
| Problem definition | Continuation of the state’s existence and protection of citizens |
| Goal | Provision of cybersecurity as a common good |
| Instruments | Expenditures, regulations, partnerships,  exchange of information, taxation, licensing, direct provision of services, no action,  contracts, subsidies and authority, penalties, etc.\* |
| Actors | Bureaucracy, elected politicians, judiciary, etc. |

\*Adapted from Mackay, 2011, 1.

Setting proactive cybersecurity policy in democracies is difficult and time consuming. Policy does and should drive operations with decisions at many different levels. With national policy set, appropriate implementation activities to carry out that policy are carried out, with ensuring continuous, proper policy enforcement and adjustments based on the circumstances (Bayuk, ix). But, in the evolution of cybersecurity, policy was left too long as an afterthought rather than the driver, leading to multiplicities in policymaking.

Overlapping constituencies create policy incompatibility. One obvious danger of decentralized systems of decision-making and policymaking is that the community and stakeholder activists who involve themselves in the management of user boards, self-governing institutions and other bodies become an unrepresentative and self-perpetuating elite. The legitimacy of governance arrangements can best be secured as a byproduct of the performance of other metagovernance functions. Legitimacy is a two-dimensional concept relating to the inputs and to the outputs of the political system. On the input side, legitimacy requires that political choices are derived, directly or indirectly, from the preferences of citizens. On the output side, legitimacy requires that organizations perform effectively. If governments effectively steer governance arrangements, ensure effectiveness and provide necessary resources, the legitimacy of the outputs is enhanced. If governments provide democratic oversight and ensure accountability, the legitimacy of the inputs is enhanced. Where, for whatever reason, governance arrangements lack legitimacy, governments come under pressure to take action” (Bell and Hindmoor, Cambridge, 2009, Rethinking Governance, 54-55). This pressure action to generate legitimacy is constant, as the ever-mounting cybersecurity incidents are. It is this continuity portion of cybersecurity policymaking we will be incorporating into the PACE model as shown below.

**3.3. Public attention and policy time scales**

In tying the public attention to the policy time scales, there is a necessity to identify policy making windows. This identification can be made by altering the definition of optimal policy windows via the Overton Window concept. The Overton Window is a concept originally introduced by Joseph Overton that acts as a measurement scale of an idea’s political viability. According to the core idea of Overton window explained by Joseph G. Lehman (Lehman 2020), if a particular proposed idea falls within the given range, the idea is likely to survive as a policy. Based on further postulation, there are different degrees of public acceptance in a given window such as an idea being seen as “radical” or “acceptable”. This approach helps identify where the ideas land within the acceptability spectrum of governmental policies.

Visual 1: Conceptual range of the Overton window of political possibility

Radical

Acceptable

Popular

Lower chance of survival

No government regulation

Total government control

**Overton Window**

Acceptable

Radical

Lower chance of survival

Source: Overton window in Collits 2020, modified by the author.

On its own, Overton model does not offer solutions to dilemmas in cybersecurity policymaking. Instead, it offers a building block in the solution framework by validating the existence of a range of political acceptability for policies. This range can be argued to be based on public interest in democratic countries where policymakers derive their legitimacy through democratically held fair elections. Unlike authoritarian regimes where only the regime continuity matters, the interests of the public drive the policymaking in democratic states. Therefore, it is within the realm of possibilities that public interest in a certain policy item can affect the relevant Overton window.

Based on this assumption, the next question becomes that of tying public interest in a certain policy topics to policy windows. Identifying optimal policy windows is the main issue for the formulation of the necessary policies at optimal timing, a common challenge faced by all states. Therefore, there is a need to formulate a framework to help solve this challenge.

Amount of public attention not equal to amount of cyberattacks. It is often the case of number of attacks being higher than the attention given. Other social events may take precedence in public attention. When the number of attacks is lower than the amount of attention given, it is possible to anticipate a few but impactful incidents occurring. Timing of the policy adaptations can be linked to the public attention and number of cyberattacks. Low intensity policies that run on a long-term basis can be introduced during the lulls such as educational initiatives and high intensity policies that run on a very short-term basis such as immediate shutdown of critical infrastructure networks can be introduced during the spikes.

Visual 2: The complete PACE Model

Time

Public attention level

**4. Applying the PACE Model to the cybersecurity policies in Japan**

In this last section, a brief application of the PACE model is given. Per the timeline of policymaking and the policy goals, the case of Japan is selected for application. Although there are multiple methods with varying effectiveness for public interest measurement such as surveys and focus groups, there is a more accessible method for measuring interest in cybersecurity offered by Alphabet Inc.’s Google search engine services. The figures supplied in the introduction were derived from this source as well the public attention figure in this section. The term was set as “cybersecurity” in Japanese (サイバーセキュリティ) with the time period between January 2004 to the end of the Tokyo 2020 Games. These dates were chosen due to the fact that Japan founded its National Information Security Center (NISC) in 2005 and that the Tokyo 2020 was a key cybersecurity policymaking area for the country.

Following the foundation of its National Information Security Center (NISC) in 2005 and the First National Strategy on Information Security in 2007 (NISC 2007), the solidification of information security, i.e., cybersecurity, as a policy area for the Japanese government was accomplished. Even with this start, Japanese government documents reveal Tokyo’s established preference to adopt a patchwork approach to enduring problems in cyberspace (Katagiri Nori, 2021). This is coupled with “... Japan government’s modest expectations demand(ing) nothing more than occasional efforts when something fundamental was going wrong” (Pan, 2005, 343).

Figure 4: PACE Model applied to a subset of cybersecurity policies in Japan, January 2004-September 2021

The time period starting from the announcement of Japan’s successful bid for Tokyo 2020 Olympics in September 2013 to the end of the games reveals heightened public attention. It was also this same time period where the PACE Model’s stipulation regarding the short-term, high-intense policy areas applies. Given the conditions surrounding policymaking, this time period was the optimal policy window for pursuing countermeasures against potential cyberattacks. This pursual was proven when the NISC announced the new cybersecurity measures being accepted in 2018 with a particular focus on the Olympics-Paralympics.

In this case of Japan’s Tokyo 2020 Games and longer term cybersecurity policymaking, the red sequoia dilemma is resolved with adaptation of a perspective that values constant pressure to engage with multiple lines of policy areas with a background of constant conflict engagements. There is not sufficient data from the case study to claim whether the PACE model’s MAD dilemma solution is fully realized. It is possible to state either that the capacity of the state need to improve more or to become more visible in the policy documents. Once the capacities are matured, the model would help in policy orientation for figurative nukes pointing required in the MAD dilemma.

**Conclusion**

Not until recently did governments eventually figure out that what they expected the policies to do in the cybersecurity area was to serve as an arena for solutions, or to put it more straightforwardly, a series of guidelines through which various actors could take precautions. This became more significant after the Stuxnet attacks when states themselves emerged as sources of more security issues. To be sure, most government leaders and policy planners are not enthusiastic about getting involved in international conflicts in cyberspace; nor do they wish to endanger their constituents. Consequently, while maintaining a low profile, they eagerly try to keep themselves well-informed on critical defense decision making.

Can better policymaking timing produce better policies? Yes, because the timing of policymaking is tied into the securitization dilemma. There is a need for sufficient level of public awareness regarding policy topics for successful securitization. Successful securitization brings successful policies, successful in the sense that the public and private sector is aware of topic and of precautions taken by the state. Optimal pairing of policymaking timing and policy window can and do occur. However, it has to be underlined that these two are not necessarily the same as the timings are not equal to policy windows due to the windows potentially created by policy entrepreneurs. Public awareness of policies and issues is often ignored as a factor.

It is important to understand the target audience of a policy in order to effectively communicate with them. Using various communication channels (internet, radio, television, print, journals, conferences, etc.) to convey the message in multiple ways, and reaching various target audiences is a part of effective policy communication. Additionally, it is important to provide the information about the policy in a way that the target audience can understand and use. Using the appropriate language for each policy target would help the audience understand why the policy is important to them, and what they should do now that they know the information.

In this study, combining time scales indicated by public attention to the understanding of constant engagement was carried out to create the PACE Model, This was done in order to point at the fact that to combat the securitization dilemma, policymakers can adapt a window of policy change. This windows also entails opportunity window for increased effective private-public cooperation. Per the results, overcoming intrinsic dilemmas in cybersecurity policymaking is found to benefit from systematic identification of optimal policy windows. Limitations of this study do exist and they are mostly soluble by further conceptual exploring of other combinations of time scales and intensity levels. With the incorporation of the case study results, overcoming intrinsic dilemmas in cybersecurity policymaking is found to benefit from systematic identification of optimal policy windows via the given model.

**REFERENCES**

Bardach, E. (2011). *A Practical Guide for Policy Analysis* (4th ed.). CQ Press College.

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). Cyber Security Policy Guidebook. In *Cyber Security Policy Guidebook*. https://doi.org/10.1002/9781118241530

Bell, S., & Hindmoor, A. (2009). *Rethinking Governance: The Centrality of the State in Modern Society*. Cambridge University Press. https://doi.org/https://doi.org/10.1017/CBO9780511814617

Cavelty, M. D., & Egloff, F. J. (2019). The Politics of Cybersecurity: Balancing Different Roles of the State. *St Antony’s International Review*, *15*(1), 37–57.

CISCO. (2020). *What Is Cybersecurity?* CISCO Homepage. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Deibert, R., & Rohozinski, R. (2011). Contesting cyberspace and the coming crisis of authority. In *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. https://doi.org/10.7551/mitpress/9780262016780.003.0002

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity Capacity: Does It Matter? *Journal of Information Policy*, *9*, 280–306. https://doi.org/10.5325/JINFOPOLI.9.2019.0280

Engerer, H. (2011). Security As a Public, Private Or Club Good: Some Fundamental Considerations. *Defence and Peace Economics*, *22*(2), 135–145. https://doi.org/10.1080/10242694.2011.542333

Gallaher, M. P., Link, A. N., & Rowe, B. R. (2008). *Cyber Security* (1st ed.). Edward Elgar Publishing. https://ideas.repec.org/b/elg/eebook/12762.html

Google Trends. (2022, March 26). *Interest over time for cybersecurity on Google, January 1, 2016-March 26, 2022*. Google. https://trends.google.com/trends/explore?date=2016-01-01%202022-03-26&q=cybersecurity

Help Net Security. (2021, February 17). *Malware increased by 358% in 2020*. Help Net Security Website. https://www.helpnetsecurity.com/2021/02/17/malware-2020/

Herzenstein, N., Marshall, A., & Soman, S. (2022, March 29). *(1) Webinar: 2022 IT Trends: Accelerating Digital Apps on Top of Traditional Systems*. GigaSpaces. https://www.youtube.com/watch?v=JKXPDhWBx7g&ab\_channel=GigaSpacesTechnologies

Hunter, L. Y., Albert, C. D., & Garrett, E. (2021). Factors That Motivate State-Sponsored Cyberattacks. *The Cyber Defense Review*, *6*(2), 111–128. https://www.jstor.org/stable/27021379?seq=1#metadata\_info\_tab\_contents

Japan National Information Security Center (NISC). (2006). *The First National Strategy on Information Security-"Toward the realization of a trustworthy society"*. https://www.nisc.go.jp/eng/pdf/national\_strategy\_001\_eng.pdf

Japan National Information Security Center (NISC). (2015). *Cybersecurity Strategy of the Government of Japan*. https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf

Japan National Information Security Center (NISC). (2018, July 27). *Cybersecurity Strategy*. The Government of Japan. https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf

Katagiri, N. (2021). From Cyber Denial to Cyber Punishment: What Keeps Japanese Warriors from Active Defense Operations? *Asian Security*, *17*(3), 331–348. https://doi.org/10.1080/14799855.2021.1896495

Kayama, K. (2015). *Kōdo hyōteki-gata kōgeki taisaku ni muketa shisutemusetsukei gaido ~ kansen suru koto o zentei to shita `bōgyo gurando dezain’ ni muketa shisutemusetsukei no kandokoro ~ (System design guide for highly targeted attack countermeasures-The key points of system design for “defense grand design” on the premise of infection-)*.

Konen, A. (2021). Quote by German Minister of Interior Andreas Konen. In *Women in Cyberspace Webinar*. Athene.

Liaropoulos, A. (2013). Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction? *Journal of Information Warfare*, *12*(2), 19–26.

Mackay, M. (2011). *Understanding and Applying Basic Public Policy Concepts*. Politice Publice. https://www.politicipublice.ro/uploads/understanding\_public\_policy.pdf

Manjikian, M. (2021). *Introduction to Cyber Politics and Policy* (1st ed., Vol. 1). SAGE Publishing. https://us.sagepub.com/en-us/nam/introduction-to-cyber-politics-and-policy/book266267

Masujima, M., & Tsuta, D. (2020). *Jirei ni manabu saiba sekiyuritei tayouka suru kiyoui eno taisaku to houmu taiou (Cybersecurity Case Studies Measures to Counter Diversifying Cyber Threats)*. Keidanren Syuppan.

Pan, L. (2005). *The United Nations in Japan’s Foreign and Security Policymaking, 1945-1992: National Security, Party Politics, and International Status*. Harvard University Asia Center. https://doi.org/10.1163/9781684174249\_001

PurpleSec. (2022). *2021 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends*. PurpleSec LLC. https://purplesec.us/resources/cyber-security-statistics/

Reich, P. C., Gelbstein, E., Wuest, M., Fridakis, S., Bosch, O., Kellermann, T., Weinstein, S., Wild, C., Cabanlong, A. S., Conway, M., Lotrionte, C. B., Ramsay, G., & Thomas, T. L. (2012). Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization. In P. C. Reich & E. Gelbstein (Eds.), *Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization*. IGI Global. https://doi.org/10.4018/978-1-61520-831-9

Shackelford, S. J. (2020). Governing New Frontiers in the Information Age: Toward Cyber Peace. In *Governing New Frontiers in the Information Age*. Cambridge University Press. https://doi.org/10.1017/9781108604000

Sigholm, J. (2013). Non-State Actors in Cyberspace Operations. *Journal of Military Studies*, *4*(1), 1–37. https://doi.org/10.1515/JMS-2016-0184

Soesanto, S. (2020). *Japan’s National Cybersecuirty Defense Posture: Policy and Organizations*. https://doi.org/10.3929/ethz-b-000437790

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. (2017). In M. N. Schmitt & et al. (Eds.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. https://doi.org/10.1017/9781316822524

The Prime Minister’s Office of Japan. (2015, March 11). *Basic Policy for Promoting Measures related to Preparations for and Management of the Olympic and Paralympic Games in Tokyo in 2020*. The Prime Minister’s Office of Japan (Shinzo Abe Administration). https://www.kantei.go.jp/jp/topics/2016/2020olym\_paralym/20160311olym\_kihonhoshin\_en.pdf

Tsuchiya, M. (2015). *Saibaa sekyuritei to kokusai seiji (Cybersecurity and International Relations)*. Chikura Shobo.

University of North Dakota, 2022. Accessed on March 24, 2022. https://www.onlinedegrees.und.edu/blog/types-of-cyber-security-threats/.

University of North Dakota B, 2022. Accessed on March 24, 2022. <https://www.onlinedegrees.un.edu/blog/types-of-cyber-attacks/>.

Velde, J. van de. (2021). When Does Election Interference via Cyberspace Violate Sovereignty? Violations of Sovereignty, “Armed Attack”, Acts of War and Activities “Below the Threshold of Armed Conflict” via Cyberspace. In D. B. Hollis & J. D. Ohlin (Eds.), *Defending Democracies : Combating Foreign Election Interference in a Digital Age* (pp. 163–178). Oxford University Press. https://lccn.loc.gov/2020039406

Waltz, K. N. (1979). *Theory of International Politics* (1st ed.). McGraw-Hill.

Yu, E. (2022, March 15). *Pandemic pushes cybersecurity to top agenda in Asean boardrooms*. ZDNet. https://www.zdnet.com/article/pandemic-pushes-cybersecurity-to-top-agenda-in-asean-boardrooms/

1. Elif Sercen Nurcan, Meiji University, Tokyo, e-mail: esnurcan@meiji.ac.jp, ORCID: 0000-0002-7104-0283 [↑](#footnote-ref-1)