States' Capacity Building for Cybersecurity: An IR Approach

Seiko Watanabe

States' Capacity Building for Cybersecurity: an IR Approach

Seiko Watanabe[1]

[1]Yokohama National University, Yokohama, Kanagawa
seikowatanabynu@gmail.com

Abstract. This paper discusses the current circumstances of security in cyberspace, such as cyber armies and cyber intelligence. Cyber intelligence plays a vital role in the balance of power. Most importantly, this paper explores previous studies of the International Relations (IR) theory of Realism. Cybersecurity can be applied as the equivalent of a nuclear deterrent of Realism and is inspired by the sense of the threat that allied countries felt in regard to cybersecurity. Countries utilize capacity building for military affairs, economics, and administration for cyber deterrence. Even though the circumstances of cybersecurity are deeply affected by the deterrence theory of Realism, concepts of capacity building for cybersecurity are derived not only from Realism but also from Liberalism and Constructivism. In the end, through this paper, I found that there is an interdependence of Realism, Liberalism, and Constructivism.

Keywords: Cyberattack, Capacity building, International relations.

1 Introduction

In recent years, the number of cyberattacks has rapidly increased, and both developing and developed nations have been unable to manage them properly because of the rapid increase in their number. This is because technologies of developing countries are not matured, and governments have been unable to catch up with the latest technology for cyber security. The intention of this paper is to describe the current situation of cyberwars and intelligence and it suggests that a sense of threat is closely tied to Realist theories of International Relations (IR). In particular, the balance of power (a Realist concept) and deterrence theory create a system of capacity building internationally. This system is well-supported by these theories, and the paper presents an analysis of the future of cybersecurity.

Many previously believed that cyberspace was an illusory world. However, in the late 2000s, nations began to notice cyberattacks perpetrated by other nations. There are two main categories of cyberattacks: (1) attacks on a nation's decision-making capabilities (intervening in elections or stealing/defacing information gathered by the government), and (2) attacks on important infrastructure (disrupting the operations of banks, hospitals, or power plants).

There are two significant examples of cyberattacks. In 2007, Estonian ministries, banks, and media suffered a serious attack by cyber terrorists, and in 2010, Iranian nuclear facilities were destroyed by two sophisticated worms, Stuxnet and Flame, which targeted and destroyed 58% of all hardware. In fact, a number of developed countries have established branch offices in developing countries; therefore, if cyberattacks occur at these branch offices, there is a high possibility that information regarding developed nations can also be stolen or damaged by cyberterrorists. Hence, developed nations need to invest in infrastructures or administrative resources to reinforce the defenses of developing countries.

2 Previous Studies of Cyberspace

2.1 Internet Intelligence and Cyberwar

John Arquilla of the US Navy's Naval Postgraduate School and David Ronfeldt of the Rand Corporation have defined cyberwar as a military operation conducted according to information-related principles. According to Richard A. Clarke and Robert K. Knake, "cyberwar" is defined as one government attacking the computers or networks of another government in order to disrupt infrastructure or steal important national security information [1]. Often, cyberwars are waged through intelligence. According to Michael Herman, intelligence activities on the Internet play a vital role in current IR [2]. The Internet allows for remote intelligence operations and keeps costs reasonably low. On the other hand, intelligence agencies are a controversial part of the modern state even though international law allows covert activity. According to Scott and Silver, accumulating information by intelligence does not contravene customary law [3-4]. In fact, Scott notes that international human rights laws do not address spying, and governments cannot apply the actual rules that were established in the Convention.

According to Jon Swartz, in 2003, hackers attacked the computer systems of NASA and Sandia National Laboratories [5], utilizing computer viruses and worms. The hackers directly accessed military and government computers and checked private and government documents [5]. In the Republic of Korea, the government, media corporations, and political parties were attacked by North Korea in June 2013. In order to prevent such attacks, intelligence communities provide information to commanders and gather, process, analyze, disseminate, and assess information. Intelligence plays a vital role, especially in times of war, as the infrastructure is heavily reliant on the capabilities of cyber forces and the infrastructure of the Internet.

Additionally, *Cyberspace and International Relations* describes how specialized military cyber forces can sneak into an opponent's central infrastructures [6]. An example of specialized military cyber forces sneaking into the infrastructures comes from Estonia in 2007. As a result of cyberattacks on the Estonian government and citizens, cash machines and online banking services were compromised, and telecommunications, transportation systems, and the power grid were destroyed [7]. Estonia was particularly vulnerable because the government and infrastructure relied heavily on the Internet. The country, an enemy of Estonia, is alleged to be behind the attack.

The most troubling aspect of the Internet is that it is an anarchic world [8]. Despite several efforts by the United Nations (UN) to bind UN member states to act reasonably and create information security [9][1], conflicts between US allies and former Soviet nations have persisted. Hence, there are no solid norms governing the Internet or holding accountable countries that act unethically.

Thus, developing nations are targeted by Internet terrorists because of their vulnerable online infrastructure [10], and developed countries often capitalize on capacity building for developing countries. The cyber-developed nations spend money on governments, infrastructure operators, cultivation of human resources, crime prevention, and technology in developing countries for the sake of international security. According to Eade and Williams, capacity building is "strengthening people's capacity to determine their own values and priorities and to organize themselves to act on these" [11]. According to Echebarria, Barrutia and Aguado [12], capacity building is derived from the UN's Local Agenda 21 and is a critically important tool for conducting a set of sustainability policies. Though often quite similar methodologies are available for preparing LA21, each municipality has its own characteristics and idiosyncrasies and must, therefore, establish its own means of acting [13]. Agenda 21 is an encompassing plan of action on the global, national, and local scales for the members of the UN and for governments and other leading groups such as non-governmental organizations (NGOs). In 1992, within the UN's Sustainable Development Goals, the Sustainable Development Knowledge Platform, Agenda 21, the Rio Declaration on Environment and Development, and the statement of principles for the Sustainable Management of Forests were agreed by more than 178 governments at the United Nations Conference on Environment and Development held in Rio de Janeiro, Brazil. The Commission on Sustainable Development was created in December 1992 to ensure effective follow-up of the conference's principles and to observe and report on the implementation of the agreements at the local, national, regional, and global levels. It was permitted that a five-year review of the progress of the Earth Summit would be conducted by a special session of the UN General Assembly in 1997. According to the Japan International Cooperation Agency, JICA, developed nations should not simply fill the gap in technology between developed and developing nations but encourage developing countries to acquire proper knowledge and foster decision making on cyber policy.

2.2 Cyber Intelligence

According to Rafal Rohozinski [14], the main objective of cyber operations is to influence or control computer networks and operate and defend friendly critical cyber infrastructure and key resources. In addition, cyber operations attack critical and hostile

[1] The United Nations Group of Governmental Experts (GGE) on "advancing responsible State behavior in cyberspace in the context of international security" (formerly: on Developments in the Field of Information and Telecommunications in the Context of International Security) is a UN-mandated working group in the field of information security. Six working groups have been established since 2004, including the GGE 2019-2021. The UN GGE can be credited with two major achievements outlining the global agenda and introducing the principle that international law applies to the digital space.

cyber assets in cyberspace, which is known as active defense. This paper proposes appropriate roles and responsibilities for cyber intelligence within cyber operations.

Cyber operations are a sequence of tactical maneuvers that have strategic cyber objectives. This includes pre-cyber task orders, such as the US Air Force's pre-air tasking order. The pre-air tasking order is defined as a procedure "used to task and disseminate to components, subordinate units, and command and control agencies projected sorties, capabilities and/or forces to targets and specific missions" for three days from the outbreak of war; it normally "provides specific instructions to include fighter call signs, targets, weapons, controlling agencies, etc., as well as general instructions." The pre-cyber task order "guides cyber-attack according to the assigned procedure at each phase in real-time" [10]. Especially, according to the book, the roles and responsibilities of cyber intelligence at respective phases of cyber operations. Cyber operations are practices related to defense, assurance, and attack [that] achieve objectives in or through cyberspace. While a cyber-operation is being conducted, cyber intelligence must properly support cyber commanders and units to ensure cyberspace intelligence superiority. Cyber intelligence is a cyber-discipline that utilizes accumulated information accumulations and analysis approaches to provide direction in decision making to cyber commanders and cyber operation units. This is a key role in cyberattack and defense. The information collected is requested by cyber commands and units and is disseminated to relevant departments. Cyber intelligence is a criticaly important factor in the cyber operations cycle.

2.3 Cyber Threats in International Relations (IR)

According to Damien McGuiness and USA Today [7, 15], cyber threats occur across academic disciplines, including the study of computers, media, literature, engineering, and policy. However, International Relations (IR) cannot catch up with the real situation and create appropriate theories, despite the present circumstance of cyberattacks being emergent. According to Eriksson and Giacomello, very few attempts have been made to apply IR theory in analyzing this development [16-18]. Research that has focused particularly on aspects of the creation of information-age security threats has not been much influenced by theory or is mostly outdated [19–22].

2.4 Cyber Wars

Thomas Rid is a prominent scholar of the risk of information technology during conflicts. His book, *Cyber War Will Not Take Place*, states that cyberwar never happened in the past, is not taking place now, and is unlikely to occur in the future. He summarized a cyberwar as comprising a potentially lethal, instrumental, and political act of force conducted through malicious code. Rid also provided nuanced terminology for cyberattacks. All politically motivated cyberattacks are merely refined versions of three activities: sabotage, espionage, and subversion [23].

Ryan Maness also mentioned what cyberattacks were. He believed that nations have a manner that is based on strategies [24-25]. Cyberattacks can yield a high return for low costs for nations. Gia also claimed that the offensive nation in a cyberattack agitates

people, creating disruptive social movements in defensive countries. There are three strategies for the nation on the offense: invalidating domains, reorganizing domains, and instigating political discord.[2]

3 Deterrence Theory and Alliances for Cybersecurity

Today, in the arena of cybersecurity, scholars have begun to consider whether the strategies used for nuclear weapon deterrence might apply to the present conflict in order to fill the gap between real cyber situations and academic research. This concept derives from the idea that any country that possesses a weapon, they are able to come under the control of an enemy, which ensures the security of the country, an idea born during the Cold War. Thomas C. Schelling stated that, at that time, both the Soviet Union and the United States had sufficient nuclear power to both threaten and deter one another [27]. This balance of power was called mutually assured destruction [28]. In deterrence theory, global political stability can be accomplished because countries know that the costs of using nuclear weapons are greater than the gains. In addition, the idea of mutually assured destruction serves as a base for the offense-defense theory, which is an essential Defensive Realist theory [29]. Defensive Realism argues that nations support the status quo to maximize the power of their political and military forces. For alliances, a nuclear umbrella is a safeguard against a non-nuclear allied state. The core idea of deterrence theory is that nations should prepare for threats and defend their allies. Despite the problem that the origin of a cyberattack cannot be known for certain because of the use of Tor, which is an anonymous modification application that disguises IP addresses, the core idea of nuclear deterrence remains the same for cyber deterrence. In both the theories of deterrence, mutually assured destruction serves as a base for the offense-defense theory, smaller allied countries can receive benefits by depending on big countries and all cooperate to ensure the safety of cyberspace: cyber-developed countries engage in capacity building for the sake of less developed countries. In the following sections, the types of capacity building are explained.

This desire to deter is a result of feeling threatened. Countries that foresee the possibility of the compromising or even destruction of their infrastructure or financial institutions or fear cyberwar ally with one another to prepare for such attacks.

[2] While these studies seem to be persuasive, the present attitude towards cyberattacks has changed since the Clinton administration. Richard Clarke, who worked with the Clinton Administration's national coordinators of international security, stated that cyberattacks from opponent nations destroy the Internet network for both citizens and government. Additionally, 9-11 was an epoch-making event for the United States and the rest of the world. The US government is concerned that major infrastructure like the Internet is a likely target for an attack [26].

4 Capacity Building

As the previous chapter indicated, capacity building is derived from the UN's Agenda 21, which aims to stabilize cyber conflict worldwide. There are three areas in which capacity building can be applied using the Grand Theory, which can entail a particular conceptualization of capacity building (Table 1).

Table 1. Capacity Building concepts

Types	Explains	Applicable IR Theory
Capacity Building for military affairs	Conducting operations, conflict prevention, and doctrine enforcement	Realism
Capacity Building for Economics	Providing financial support to share the same Internet infrastructures	Liberalism
Capacity Building for administration / norms of law enforcement	Helping developing countries' systems of law enforcement	Constructivism

4.1 Military Capacity Building

According to David Guy, a researcher at the Australia Strategic Policy Institute, building military capacity aims to enforce armed exercises, prepare for cyber-attacks from enemies, conduct operations, prevent conflict, and enforce doctrine, which is same as traditional Realism. Martin Hall has written "Realist theories, have indeed been put to use by the armed powers" [32]. According to Prashanth Parameswaran in The Diplomat [32], Association of Southeast Asia Nations (ASEAN) states cooperate with Japan to boost their cyber capabilities. In fact, Singapore's new ASEAN Cyber Capacity Program was announced at the inaugural ASEAN Ministerial Conference on Cybersecurity in October 2016 [33]. The Philippines also announced the launch of a cybersecurity working committee within the ASEAN Defense Ministers Meeting Plus in 2016. Another key movement for cyberspace is the ten-million-USD ASEAN Cyber Capacity Programme (launched by Singapore in 2016). This program enhances cybersecurity expertise across the region. In order to pursue a peaceful cyber world, the program also launched the Singapore-ASEAN Cybersecurity Centre of Excellence in 2019. The center is based in Bangkok at the ASEAN-Japan Cybersecurity Capacity Building Centre, launched in September 2018, which seeks to prevent cyberattacks. Almost 700 of the cybersecurity personnel who work there are from Southeast Asia and have graduated from Japanese-designed programs that include instruction in cyber defense, digital forensics, and malware analysis [34].

4.2 Economic Capacity Building

Capacity building for economics is primarily digitalization support, which is believed to enhance a nation's economy. This idea is derived from Liberalism, an IR concept. In

Liberalism, scholars believe that economic interdependence greatly influences nations' relations. According to Robert Gilpin, "liberalism assumes that a market arises spontaneously in order to satisfy human needs [32]. Capacity Building also tries to satisfy citizens demands by aiding cyber infrastructures from developing countries to developing nations. For example, the United Kingdom has contributed to the economy of the Commonwealth through cyberspace capacity building in accordance with the Sustainable Development Goals. The United Kingdom invests in cybersecurity in developing countries, assuming that they will be able to utilize the technology by themselves [35]. By promoting investment and trade of goods and services in the Commonwealth through democracy and fair competition not only have Commonwealth countries benefitted, but the UK has as well. The UK government enhances the importance of building resilient digital economies and needs of ITC investments to commonwealth countries [36]. Also, the UK government invest partnership in Africa, Asia, the Pacific and the Caribbean for improving digital economies [37].

The United States has helped Nigeria to prosecute an international cyber-fraud scheme. Ayofe and Oluwaseyifunmitan [38] suggested that the erection of a structure for the implementation of information assurance in critical sectors of the economy (such as public utilities, telecommunications, transport, tourism, financial services, the public sector, manufacturing, and agriculture) and developing a framework for managing information is necessary for cyber-developing countries. According to Niels Schia [39], cyber capacity building and digitalization of the economy are deeply connected.

4.3 Normative/Administrative Capacity Building

Capacity building for administration and norms aids developing countries' systems of law enforcement, which deeply connect to an idea of Constructivism, a concept of International Relations (IR). According to Nicholas Greenwood Onuf, the Constructivists believe that rules is important for society. Governed rules give people perspectives about how they should behave in a society[40].

In fact, developing countries want to improve law or rules of cyber security in developing countries through Capacity Building. For instance, the Estonian government, which is a cyber-developed country, emphasizes the importance of capacity building for fighting cybercrime, and it introduced the European Council Convention on Cybercrime (also known as the Budapest Convention) to developing countries [37]. Estonia and partner institutions from the United Kingdom and the Netherlands have been supporting the cyber development of countries in Africa and Asia. The Cyber Resilience for Development project will last until June 2021; the project appears in the cybersecurity yearbook published by the Estonian Information System Authority. According to the Estonian government, [41], "the activity has been launched in Mauritius, Sri Lanka, Ghana, and Botswana. The purpose of the mission is to increase awareness about cybersecurity, help develop cyber strategies and action plans, enhance the capability of the teams for handling cyber incidents, and share the experience with providers of vital services and institutions of the state" [42]. In addition, enhancement of computer security and incident response teams, protection of critical information infrastructure and regulation, risk management and crisis exercises, cyber-related laws and strategies, and

cyber hygiene and awareness have been strategically established. Sri Lanka and Mauritius have demonstrated an interest in Estonia's experiences with dramatic growth through e-government. The Estonian government incorporates with the State Infocommunication Foundation (RIKS), and a consortium of private sector companies, including Cybernetica, Dell EMC, Ericsson, OpenNode, and Telia (Resource: e-governance, e-estonia,).

5 Future Implications: GGE and Capacity Building

In spite of the continuing policy of Realism in cyber security and the state of anarchy, there is a tendency towards cooperation among nations in the UN. A Group of Governmental Experts on advancing responsible state behavior in cyberspace in the context of international security was established in 2004. According to the UN website, the members of the GGE countries are Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco, Netherlands, Norway, Romania, Russian Federation, Singapore, South Africa, Switzerland, United Kingdom, United States, and Uruguay [43]. The GGE is planning to hand in its final report to the UN in 2021. Sash Jayawardane, Joris Larik, and Erin Jackson states that GGE is now trying to determine how existing international law can be applicable to cyberspace [44]. Especially, in the GGE, the above nations discuss how international law can be applied to cyberspace. Also, GGE countries support Capacity Building [45]. In the near future, there is a great possibility that nations conduct capacity building while appreciating benefits of rules of GGE.

6 Limitations

The intent of this paper is to analyze categorical translation into realism, liberalism, and constructivism, while applying capacity building to the aforementioned theories. However, in the field of IR, some important studies examining realism, liberalism, regime theory, and global governance already exist. This paper fails to specifically mention regime theory and global governance theory. Furthermore, research on regime theory considering capacity building in cyber spaces already exists, and some scholars have already analyzed this in terms of global governance such as the Paris Call, Commission on the Stability of Cyberspace report. It is necessary to employ these studies and have an independent discussion as well. Global governance is a critical philosophy that relates to the GGE and other Internet regimes. In a future academic thesis, I would like to include regime theory and globalization theories in a comprehensive theory for a better discussion of cyber security.

7 Conclusion

This paper introduces a general description of the types of cyberattacks and discusses previous studies of Internet intelligence, cyberwar, and theory for cyberspace. According to previous studies, nuclear deterrence can be applied to incidents of cybersecurity. Such deterrence still applies to the present situation even though attribution problems exist that make identifying the source of a cyberattack almost impossible. In response to these circumstances, nations cooperate in cybersecurity efforts through capacity building. To illustrate capacity building clearly, this paper analyzed military, economic, and normative concepts of capacity building through example cases by applying the IR Theories. The cybersecurity field is still quite new, but scholarly work in the field is needed to prevent conflict in cyberspace. Especially, capacity building is quite useful to the present situation. There are three definitions of capacity building for cyber threats: Realism, Liberalism and Constructivism, which are core ideas of IR. The most important finding in this article is that the IR ideas of Realism, Liberalism and Constructivism exist in capacity building of cyber.

References

1. Clarke, R.A.: Cyber war: The next threat to national security and what to do about it. Tantor Media, Oxford (2014).
2. Herman, M.: Intelligence power in peace and war. Cambridge University Press, Cambridge (1996).
3. Scott, R.D.: Territorially intrusive intelligence collection and international law. AFL Rev. 46, 217 (1999).
4. Silver, D.B.: Intelligence and counterintelligence. In: Moore, J.N., Turner, R.F. (eds.) National security law. 2nd edn. pp. 935–965, Carolina Academic Press, Durham (2005).
5. Swartz, J. Chinese hackers seek U.S. access. USA Today Education. (2007, March 12). http://www.usatodayeducate.com/wp-content/uploads/chinese.pdf
6. Kremer, J.-F., Müller, B. (eds.): Cyberspace and International relations: theory, prospects, and challenges. Springer-Verlag Berlin Heidelberg, London (2014).
7. McGuinness, D.: How a cyber attack transformed Estonia. BBC News. (2017, April 17). https://www.bbc.com/news/39655415
8. Ludlow, P.: Crypto anarchy, cyberstates, and pirate utopias. MIT Press, Boston (2001).
9. Geneva Internet Form, UN GGE and OEWG, https://dig.watch/processes/un-gge, last accessed year/month/date.
10. Eom, J.-H. Roles and responsibilities of cyber intelligence for cyber operations in cyberspace. International Journal of Software Engineering and Its Applications 8(9), 137–146 (2014).
11. Eade, D., Williams, S.: The Oxfam handbook of development and relief. Oxfam, Oxford (1995).
12. Echebarria, C., Barrutia, J.M., Aguado, I.: Local agenda 21: progress in Spain. European Urban and Regional Studies 11(3), 273–281 (2004).
13. Valentin and Spangenberg, 2000
14. Rohozinski, R.: The new reality of cyberwar: prospects and challenges. Taylor & Francis, Oxford (2012).

15. Cybersecurity, Is cybersecurity a key component of our nation's homeland security?: US efforts to secure the information age, USA Today Education, http://www.usatodayeducate.com/wp-content/uploads/chinese.pdf
16. Eriksson and Giacomello 2006
17. Giacomello and Eriksson 2007
18. Latham 2003
19. Bendrath 2001
20. Bendrath 2003
21. Eriksson 2001b
22. Bendrath et al. 2007
23. Rid, T.: Cyberwar will not take place. Journal of Strategic Studies 35(1), 5–32 (2012).
24. Ryan, C.M. Cyber strategy: the evolving character of power and coercion. Oxford University Press, Oxford (2018).
25. Herrera, G.L.: Cyberspace and sovereignty: thoughts on physical space and digital space. Paper presented at the 1st International CISS/ETH Conference on "The Information Relations and the Changing Face of International Relations and Security," Lucerne, Switzerland, May 23–25, 2005), p. 30 (2005).
26. Min, K.-S., Chai, S.-W., Han, M.: An international comparative study on cybersecurity strategy. International Journal of Security and Its Applications 9(2), 13–20 (2015).
27. Schelling 1960, p. 207
28. Schelling 1960, p. 207
29. van Evera 1998, p. 6
30. Hinkle, R.C.: Developments in American sociological theory, 1915-1950. SUNY Press, Albany (1994).
31. Bridgman, P.W.: The logic of modern physics. New York, Macmillan (1927).
32. Hall, M.: Constructing historical realism: international relations as comparative history. Lund University (1999).
33. Parameswaran, P.: Japan-ASEAN cyber cooperation in the spotlight. The Diplomat (2017, February 24). https://thediplomat.com/2017/02/japan-asean-cyber-cooperation-in-the-spotlight/
34. Tanakasempipat, P.: Southeast Asian cybersecurity center opens in Thailand. Reuters (2018, September 14). https://www.reuters.com/article/us-asean-cyber/southeast-asian-cyber-security-center-opens-in-thailand-idUSKCN1LU1G0
35. Commonwealth Cyber Declaration, https://thecommonwealth.org/commonwealth-cyber-declaration, last accessed 2020/01/31.
36. UK Government.: UK programme supporting cyber security in the Commonwealth: call for expressions of interest, https://www.gov.uk/government/publications/uk-programme-supporting-cyber-security-in-the-commonwealth-call-for-expressions-of-interest, last accessed 2020/02/19.
37. Global Cyber Security Capacity Centre: Global Impact Knowledge and Policy Contributions from the First Five Years. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/GCSCC%20booklet%20WEB.pdf#search=%27UK++partnership+in+Africa%2C+Asia%2C+the+Pacific+and+the+Caribbean+cyber%27
38. Ayofe, A.N., Oluwaseyifunmitan, O.: Approach to solving cybercrime and cybersecurity. International Journal of Computer Science and Information Security 3(1), (2009).
39. Schia, N.: Cybersecurity capacity building, digitalization, and the Global South. European Cybersecurity Journal 2, 82–94 (2016).
40. Onuf, N.G.: World of our making: rules and rule in social theory and international relations. Routledge, New York (2013).

41. Plantera, F.: Estonia takes on a major role in cyber diplomacy with a new department for international cooperation. E-estonia (October 2019). https://e-estonia.com/estonia-cyber-diplomacy-international-cooperation/
42. Baltic News Service. Estonia supports developing cybersecurity in 4 countries of Africa, Asia. Leta. (2019, April 2). https://leta.lv/eng/defence_matters_eng/defence_matters_eng/news/4D29207F-14E5-4490-8973-F830B28E5C37/
43. United Nations Office for Disarmament Affairs. Group of Governmental Experts, https://www.un.org/disarmament/group-of-governmental-experts/, last accessed year/month/date.
44. Jayawardane, S., Larik, J., Jackson, E.: Cyber governance: challenges, solutions, and lessons for effective global governance. The Hague Institution for Global Justice (2015). https://www.thehagueinstituteforglobaljustice.org/wp-content/uploads/2015/12/PB17-Cyber-Governance.pdf