International Journal of Social Sciences Bulletin
Volume 2, Issue 4, 2024 ISSN: (E) 3007-1917 (P) 3007-1909

CYBER CONFLICT AND INTERNATIONAL ORDER THE SYSTEMATIC ANALYSIS OF CYBER WARFARE TRENDS AND THEIR IMPACTS

Muhammad Bilal Shakeel[*1], Muhammad Tahir[2], Imran Kazi[3], Mubashra Sattar[4], Shiv Ram Ashraf[5], Arshiya Tariq[6], Muhammad Asif[7]

*[*1]Department of Political Science and International Relations, University of Sargodha*
[2]Graduate School of Science and Engineering (Electronics), Karachi Institute of Economics and Technology (KIET), Karachi, Pakistan
[3]Ketner School of Business, Trine University
[4]Australasian Academy of Higher Education, 363 King St, West Melbourne, Victoria, 3003, Accredited Institute of Higher Education, Australia
[5]Allama Iqbal Open University Islamabad, Department of Business Administration
[6]Graduate School of Science and Engineering, Federal Urdu University Arts, Science and Technology (FUUAST), Karachi, Pakistan
[7]Department of Pakistan Studies, Imperial College of Business Studies, Lahore

[*1]bilalshakeel241581@gmail.com

Corresponding Author: *

Received	Revised	Accepted	Published
02 November, 2024	02 December, 2024	17 December, 2024	25 December, 2024

ABSTRACT

The scope of cyber warfare practices and the deep implications to the global international order, are thoroughly reviewed systematically. The focal point is on understanding how cyber operations are changing state interaction, security dynamics and the geopolitics of the digital age. The review was based on ten foundational articles, and a comprehensive literature selection process was based on databases including JSTOR and Google Scholar to name a few, with emphasis placed on varied themes like cyber diplomacy, national security through cyber security strategies, and international law challenges. Insights on how cyber deterrence, digital sovereignty play, and the gaps in international policy frameworks are extracted through thematic coding and narrative synthesis. It finds that cyber warfare has become a high priority instrument of statecraft, used by nations to shape the global power balance and secure strategic advantage. The same can be illustrated with case studies of such incidents as the 2007 Estonian cyber-attacks, U.S.- China cyber tensions and Iranian cyber tactics and demonstrates the complex strategies states employ and why international norms should be cohesive. Without a unified approach to cyber governance, the risks of geopolitical escalation and instability will grow, the review concludes. This analysis emphasizes the importance of creating strong and internationally recognized cyber security policies to establish a stable, cooperatively ordered international environment as the cyber conflict escalates.

***Keywords**: Cyber warfare, international relations, digital sovereignty, cyber security policy, global stability.*

INTRODUCTION

Consequently, cyber warfare has completely adapted to the global environment in a growing way, and has become a major factor in contemporary geopolitics (Lehto, 2018). Now working as powerful tools to states to project influence, disrupt adversaries and protect national interests, cyber operations have become far more sophisticated. Now, cyber warfare has become a major part of national security and can no longer be only military related, it can also have impact on economic, political and societal domains. Cyberspace has become a domain of international competition with new opportunities for strategic advantage, but with new vulnerabilities and risks. The evolution of cyber warfare from the high profile incidents of 2007 in Estonia, the U.S. China cyber tensions and Iran's cyber operations has brought cyber warfare from a new front that no one imagined to a global threat that fundamentally altered how international conflict occurs (Czosseck et al., 2011).

Therefore, given the ongoing technological and geopolitical transitions, this systematic review is important. Both policymakers, diplomats and security strategists will need to understand implications of this ever more prevalent form of cyber warfare. This review studies the evolution of cyber conflict and its effect on international relations, and seeks to achieve comprehensive understanding of the strategic dimensions of cyber warfare. A serious gap in policy and governance is revealed by the literature, which is a poignant reminder that there are insufficient cohesive international normative and regulatory screens that govern cyber activities. Also, the paper discusses the growing fear of being digital sovereign as nations try to grab their cyber space to separate the global Internet into pieces. If the international policies are to be shaped successfully, diplomacy is to become productive and geopolitical stability is to be maintained, then these dynamics have to be understood.

To systematically analyze the range and the strategic dimension of cyber warfare and assess its influence on the global international order are the major objectives of this review. It includes learning how cyber warfare is a statecraft tool and its impacts on power dynamics, its implications to international security and diplomacy (Whyte, 2015). It also examines gaps in current international policies and framework associated with cyber warfare and exploration of future research avenues. The review explores the challenges and opportunities of cyber warfare in the evolving international system through a review of key case study cyber incidents such as Estonia, China and the United States as well as theoretical perspectives of cyber conflict.

Methodology

A systematic approach to literature search was adopted so as to exhaustively search the topic. These articles were collected from different academic databases Google Scholar, JSTOR, IEEE Xplore and Taylor & Francis. The reasons for selecting these databases are that they have extensive collection of scholarly articles, especially articles related to international relations, cybersecurity and digital governance.

Key words employed were "cyber warfare", "cyber diplomacy", "cyber security policy", "international law", "state sponsored cyber-attacks" and "digital sovereignty" (Hunter et al., 2021). Using these targeted keywords, it made sure that the review had covered articles discussing the geopolitical, legal and strategic sides of cyber warfare, and a clear picture of the current topic has been presented.

However, certain inclusion criteria were set to sustain a very high level of relevance and focus. Articles were included if they deal with such topics as state sponsored cyber-attacks, international cyber laws, national cyber security strategies, cyber deterrence, and digital sovereignty. Priority was given to studies that helped provide insight into the relationship between cyber warfare and international relations or on case studies of famous cyber incidents.

Instead, studies that dealt exclusively with technical aspects of cyber security, such as encryption algorithms, network security protocols or only technical threat assessments, with no geopolitical or strategic context, were

excluded as exclusion criteria (Scarfone et al., 2008). That resulted in the review focusing on the international and policy implications of cyber warfare.

Data Extraction and Analysis

Data collection involved determining The strategic dimensions of cyber warfare were systematically coded based on key themes such as cyber deterrence what information is relevant from which selected articles by thematic coding (Robinson et al., 2015). The strategic dimensions of cyber warfare were systematically coded based on key themes such as cyber deterrence, cyber diplomacy, international legal 'frameworks' and state behaviour in cyberspace and defined. By extracting this qualitative and quantitative insight, we were able to provide important insight into the more general effects of cyber operations on global stability.

This review utilized the Synthesis Approach of a narrative synthesis of geopolitical, legal, and strategic themes. Thematic analysis resulted in identification of common patterns, divergence and key gaps within the literature (Braun & Clarke, 2022). A review synthesizing variety of information brings a holistic perspective to how cyber warfare is pertaining to and intermingling with, the developments of international relations, as well as the difficulties and challenges the international community faces in regulating cyber activities as well as preserving global security.

Historical Overview of Cyber Warfare

Evolution of Cyber Warfare

There have been many incidents in the evolution of cyber warfare to prove that cyber warfare is playing an increasingly larger role in international conflict. Among the many such attacks was the 2007 cyber-attacks on Estonia—at one point targeting nearly 70 percent of Estonian government websites, and often cited as the first major case of cyber warfare in action, highlighting the ability of cyber operations to impose political effects, and disrupt national infrastructure (Mazanec, 2015). With this, state and non-state actors could start using cyber to achieve strategic objectives, and the era of warfare started. But as cyber warfare has expanded to encompass a suite of tactics, including espionage, disinformation campaigns and destructive attacks on critical infrastructure, not every state has necessarily had the tools to counter the burgeoning sophistication and speed of cyber threats. Recent U.S.-China cyber tensions mark the more sophisticated and the increased scale of cyber operations, and call for robust international framework to manage such threats.

Milestones in Cyber Conflict

Stuxnet, Solar World and the Sony Pictures' hack are key events in the history of cyber conflict. One such weapon: the attack known as Stuxnet on Iran's nuclear facilities was followed by a realization that cyber weapons could damage processes and hardware that can change the world, driving the lines between cyber and conventional war. SolarWorld hack, known to be at the hand of Chinese state actors, shook cyber espionage as a way of obtaining economic and technological preponderance (Uniacke, 2019). For example, during Sony Pictures hack, allegedly perpetrated by North Korea, cyberattacks gained a new lease on life as a weapon of coercion and intimidation, with an added difficulty in determining how to respond internationally to the threat.

Theoretical Perspectives on Cyber Warfare

Realism and State Sovereignty

Realistically, cyber warfare is a way for states to become powerful and keep their sovereignty. States can project power without direct military engagement; cyber capabilities offer a low cost way to attain strategic goals. Anarchic realism focuses on the validity of the idea that the sovereign international system is anarchical and states as 'units' only seek their own security and interests. Now, in this sense, cyber warfare becomes an extension of state sovereignty, permitting nations to fight back against perceived attacks, and reassert their dominance online (Franzese, 2009).

Liberal Institutionalism and Cooperation

At the other extreme, liberal institutionalism studies the likelihood of cooperation via the introduction of norms and treaties. As an emerging field, cyber diplomacy looks to build frameworks to reduce risk of cyber conflict and promote cyber stability. But based on international agreements such as the United Nations Group of government Experts (UNGGE) on cybersecurity, states are trying to establish shared norms and build trust (Davis & Lewis, 2019). Traditional liberal institutionalism emphasizes the need to counter challenges induced by cyber warfare with the use of multilateral cooperation, and the need to formulate international laws and protocols for the management of cyber threats.

Constructivism in Cyber Threat Perception

Through the constructivist lens, we have been arguing that norms, identity, and perception are the factors that shape states' understanding and response to cyber threats. The understanding of cyber threats is shaped by a state's identity, historical experience, and its link with other actors. For instance, the way that cyber incidents are framed as acts of aggression or espionage can differ greatly between states which will lead to variations in their response and policy issues. Social constructs in defining the nature of cyber conflict and the acceptable behavior in cyberspace is the key message that comes out of constructivism approach (Eriksson & Giacomello, 2014).

Case Studies of Major Cyber Incidents

Estonia 2007

Widespread as they are, the 2007 cyber-attacks on Estonia are considered the first major case of state sponsored cyber warfare. Attacks were directed against government, financial and media institutions, which severely impacted a state. This case demonstrated that national infrastructure is vulnerable to cyber-attacks and therefore needed to be more secure. NATO's action also made cyber defense an integral part of collective security, so NATO created the NATO Cooperative Cyber Defense Center of Excellence (Efthymiopoulos, 2019).

U.S.-China Cyber Tensions

The United States and China have been battling cyber tensions, characterized by accusations of state sponsored espionage and intellectual property theft. And both nations have waged cyber operations as a matter of course to gain strategic advantages; the U.S. to deflect Chinese cyber espionage activities, and China to bolster technological and economic capabilities. The 2015 U.S.-China Cybersecurity Agreement was one of a number of diplomatic agreements meant to lower the temperatures in cyber but it has faced enforcement and attribution challenges (Efthymiopoulos, 2019).

Iranian Cyber Tactics

Cyber has become a key and growing tool for Iran to expand its influence, and to cope with political pressure. One of Iranian cyber tactics has been its appearance in the attacks on the critical infrastructure in neighboring countries or the disinformation campaigns against regional adversaries to destabilize them. In this way, cyber warfare has played a part in increasing instability in the Middle East as a whole, while explaining how regional power dynamics are forged.

Table 1: Notable Cyber Operations and Their Strategic Implications in Global Politics

Year	Actors Involved	Targets	Outcomes	Strategic Significance
2007	Alleged Russia	Estonia (Government, Financial)	Increases in NATO cyber cooperation	This was a big escalation in Cyber operations.
2010	USA, Israel	Iran (Nuclear Facilities)	Damaged Iranian centrifuges	First known cyber weapon that creates physical damage

2015	Alleged North Korea	Sony Pictures	Data leak, financial and integrity damage	It highlighted how cyber-attacks are used for coercion.
Various	China	U.S.Corporations(Solar World)	Intellectual property theft	Economic espionage with strategic gains
Ongoing	USA, China	Various governmental institutions	Espionage, counter espionage, diplomatic tension.	Cyber tensions that continue to affect global politics
Ongoing	Iran	Middle East regional adversaries	Infrastructure disruptions, political destabilization	A part of broader regional power dynamics

Technological Developments in Cyber Warfare
Rise of Digital Sovereignty

Nations are now trying to develop and shape their cyberspace and this concept of 'digital sovereignty' has come to the fore. China and Russia, for example, have played a hand in pushing policies that attempt to ramp up state control of the Internet with the goal of defending their digital infrastructure from attacks from the outside world and articulating state sovereignty in Cyber space (Polyakova & Meserole, 2019). This trend towards digital sovereignty poses implications to the openness and interoperateability of the global Internet and maybe lead to a fragmented digital society.

Cyber Weaponry and Cyber Deterrence

Many nations have taken the priority position of developing offensive and defensive cyber capabilities. Cyber weaponry is comprised of tools to sabotage, harm, or destroy digital systems, or cyber deterrence is about preventing attackers from carrying out cyber-attacks by making them demonstrate the capacity of retaliation (Rid & McBurney, 2012). The effectiveness of cyber deterrence remains a subject of debate, because attribution is a challenge, and because cyber threats are evolving. But national security in the digital age demands development not just of offensive, but defensive capabilities, as well.

Strategic Impact on International Relations

Cyber Deterrence and Strategic Balance

Due to cyber warfare becoming a factor that changes the balance of forces in international relations it has become part of national security. In its purest sense, cyber deterrence is the ability to prevent adversaries from launching cyber-attacks by showing that potential for significant retaliation. At the same time, however, like all deterrence, cyber deterrence is complicated by the challenge of attribution in cyberspace along with the anonymity of actors in the cyber domain itself (Lupovici, 2016). Offensive cyber capabilities alone have been created by nations as a way to defend against attacks and as deterrence to hostile groups. This strategic shift has transformed power dynamics as both state and nonstate actors are using cyber to disrupt power equities and disrupt normalcy without the use of traditional fighting.

Cyber Sovereignty vs. Open Internet

Since then, one of the major issues of international relations has been that of keeping the Internet open, global and at the same time assert cyber sovereignty. China and Russia advanced some nations' agenda to gain even more control over their domestic cyberspace, thereby moving toward a fragmented Internet consistent with political and security interests (Ebert & Maurer, 2013). These principles run into challenges to the idea of a free and open Internet as this movement toward digital sovereignty protects national security, helps deter foreign influence. This international collaboration on cybersecurity issues has been seriously stunted by the divergence between countries in favor of cyber sovereignty and countries in favor of an open Internet.

Policy Adaptations and International Law

Development of Cyber Norms

A significant part of efforts to control state behavior in cyberspace has been the development around international cyber norms. A prominent contribution to the subject is the Tallinn Manual, a document produced by international legal experts help explain the use of international law in cyber warfare (Kessler & Werner, 2013). The Tallinn Manual notwithstanding, its adoption was not legally binding, however, it has been at playing a crucial role in the formation of the discourse on how otherwise valid international law should be applied to cyberspace. This provides a basis for thinking about what states need to do responsibly in the cyber domain, namely being transparent, accountable and respecting sovereignty. The norms here seek to preclude the risk of conflict with associated uniform baselines for state action, which serve to increase stability in international affairs.

Despite progress in norm development in cyberspace, there remain wide gaps in international cyber law. Lack of universally accepted definition of cyber aggression makes it very difficult for states to be held accountable for malicious cyber activities. The blurred nature of cyber actions, and their occurrence below a threshold of traditional armed conflict, makes it difficult to apply existing legal frameworks.

Additionally, technological advancements occur at a breakneck pace and involve nonstate actors, and due to insufficient attention of international law, extremely important regulatory voids are left open to adversaries. To address these challenges, a more comprehensive development of more comprehensive international legal standards is needed to deal with the peculiarities of cyber warfare (Watney, 2014).

The Role of Cyber-Diplomacy

Bilateral Cyber Agreements

Cyber agreements have been emerging as a method through which to manage tensions and mitigate the probability of conflict in cyberspace on a bilateral basis. For example, one that comes to mind is the 2015 U.S.-China Cyber security Agreement, drafted to reduce cyber enabled economic espionage and build trust between the two nations (Keitner & Clark, 2019). Despite being a big step towards cyber peace, the effect of the agreement has been weakened by concerns of verification, enforcement, and in particular the geopolitical tension between the United States and China. These agreements put between the lines the value of diplomacy in managing cyber relationships, but they also tell of the pitfalls of permanent guarantees in an environment of distrust and rivalry (Shackelford et al., 2015).

Multilateral Frameworks

Bilateral efforts have been complemented by multilateral frameworks to tackle much larger questions of how to deal with the cyber threats. Fostering international dialogue and forwarding systems of reasoned national and international cyber security that include, among others, NATO, UN, and the EU. For example, NATO has incorporated cyber defense as an organizing principle within its collective security mandate – in short, NATO has accepted that cyber-attacks may constitute triggers for Article 5. Likewise, the UN has also been building on the work emerging from the GGE on 'establishing norms of responsible state behavior in cyberspace'. Promoting international cooperation and a unified response to the increasing risk of cyber warfare are absolutely vital and these multilateral efforts are a key part of that. A diversity of interests among member states however can hinder consensus building, making it difficult particularly for such international agreements to be operated within a cohesive mode (Hughes, 2009).

Future Trends in Cyber Warfare

Emerging Threats

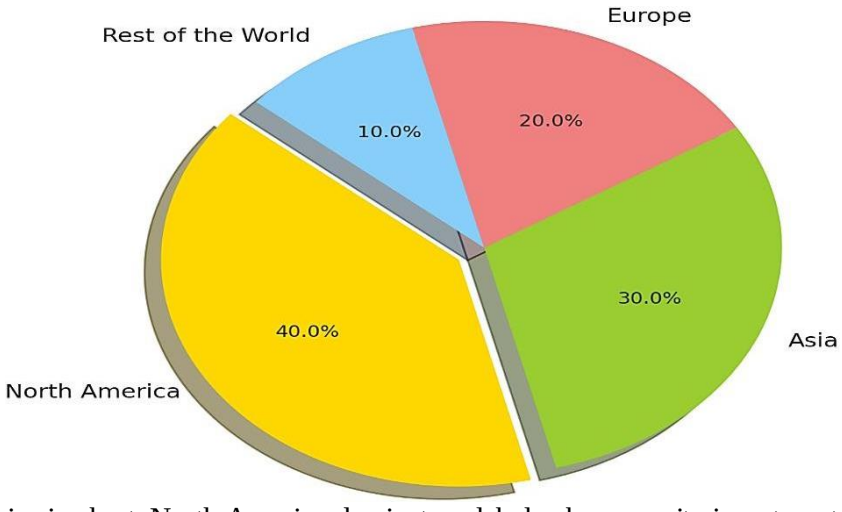
New challenges to international security are likely to be posed by emerging threats of cyber warfare. In my opinion we will see more sophisticated and targeted cyberattacks launched against us by state and non-state actors as a result of advances in technologies such as AI, quantum computing and 5G networks. For

example, AI could enable faster and more accurate attacks which are harder to spot and oppose (Brundage et al., 2018). If this technology is actually developed and implemented, then encryption could soon become obsolete, and data security would render the current encryption methods completely obsolete. The expansion of the Internet of Things (IoT), therefore, doubles the attack surface, brings more entry points for our cyber adversaries (Makhdoom et al., 2018). Using predictive analysis, it predicts that these trends will not only continue to raise the frequency of cyber incidents, but also the impact, and proactive measures will be needed to boost resilience.

Strategic Recommendations

In order to respond to the emergent realities of cyber warfare, a set of strategic recommendations are offered to further strengthen resilience and advance international cooperation. First, countries should invest in building strong cyber defense infrastructure in the form of advanced detection and response capabilities, as measures to decrease the negative effect of cyber-attack. Second, we need to work together more internationally to put in place more comprehensive, legally based frameworks to address the specific problems of cyber warfare. It concerns the elaboration of norms of cyber aggression and defining the understanding of international humanitarian law in relation to cyberspace. Third, public private partnerships need to be promoted, as much of the critical infrastructure being targeted by cyber-attacks is privately owned (Carr, 2016). It's a matter of governments and private sector entities having to begin working with each other to share threat intelligence, to come up with best practices, and improve upon their overall cyber resilience. Capacity building initiatives are essential for making everyone resilient in their preparedness for the cyber security risks. Part of that includes improving the technical skills and capacity of government agencies, the private sector and civil society to mitigate and countervail cyber threat. Through investing in member countries' training programs, international cooperation and knowledge sharing initiatives, countries can increase members' resilience to cyber-attacks, and create a safer and more stable cyberspace (Wing, 2004).

Figure 1: Cyber security investment by region



As can be seen in this pie chart, North America dominates global cyber security investments while Asia, Europe and the Rest of the World follow behind (Heinl, 2014)

Conclusion

The emergence of cyber warfare and the change in its role playing in reshaping international relations have also been discussed in this review, implications of which for global stability and security are significant. Key findings are about the use of cyber capabilities by the states strategically, digital sovereignty dispute as a contested issue, and

challenges posed due to absent cohesive international norms. The growth of cyber warfare over issued events like Estonia 2007 attacks Stuxnet and the US China cyber tensions illustrates the need of strong international frameworks to curb these threats. This review's findings enrich our understanding of international relations theories in relation with cyber warfare. Through an emphasis on state power and sovereignty in cyberspace, realism reaffirms itself, while liberal institutionalism makes a case for cooperation in cyber space through cyber norms and treaties. It offers theoretical insights as to why perceptions and social constructs determine state behavior in cyberspace and how shared norms decrease the probability of conflict. The review for policymakers shows that they need to take stronger measures to improve global cyber security with the passage of comprehensive legal frameworks and international norms. With these challenges to attribution, enforcement and rapid pace of technological advancement, it is important to have well defined cyber aggression and international collaboration. Improving cyber resilience and achieving a coordinated response to new threats also requires the use of public private partnerships and capacity building initiatives. The gaps revealed in the current literature should be considered in future research to address areas, including the need for the development of universally accepted norms for cyber engagement. The development of effective mechanisms of attribution and accountability, and the exploration of the consequences that the currently emerging technologies (e.g. AI and Quantum computing) can have on cyber warfare would require further exploration. Finally, comparative studies of the success of various national cyber security techniques could be useful to policy makers when they need to strengthen their cyber defense

REFERENCE

Braun, V., C Clarke, V. (2022). Conceptual and design thinking for thematic analysis. Qualitative psychology, S(1), 3.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., C Filar, B. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv preprint arXiv:1802.07228.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. International Affairs, S2(1), 43-62.

Czosseck, C., Ottis, R., C Talihärm, A.-M. (2011). Estonia after the 2007 cyber-attacks: Legal, strategic and organisational changes in cyber security. International Journal of Cyber Warfare and Terrorism (IJCWT), 1(1), 24-34.

Davis, J. A., C Lewis, C. (2019). Beyond the United Nations Group of governmental experts. The Cyber Defense Review, 161-168.

Ebert, H., C Maurer, T. (2013). Contested cyberspace and rising powers. Third World Quarterly, 34(6), 1054-1074.

Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. Journal of Innovation and Entrepreneurship, 8(1), 12.

Eriksson, J., C Giacomello, G. (2014). International relations, cybersecurity, and content analysis: a constructivist approach. The Global Politics of Science and Technology-Vol. 2: Perspectives, Cases and Methods, 205-219.

Franzese, P. W. (2009). Sovereignty in cyberspace: Can it exist. AFL Rev., c4, 1.

Heinl, C. H. (2014). Regional cybersecurity: moving toward a resilient ASEAN cybersecurity regime. Asia policy(18), 131-160.

Hughes, R. (2009). Towards a global regime for cyber warfare. In The Virtual Battlefield: Perspectives on Cyber Warfare (pp. 106-117). IOS Press.

Hunter, L. Y., Albert, C. D., C Garrett, E. (2021). Factors that motivate state-sponsored cyberattacks. The Cyber Defense Review, c(2), 111-128.

Katin-Borland, N. (2016). Cyberwar: A real and growing threat. In Cyberspaces and Global Affairs (pp. 3-22). Routledge.

Keitner, C. I., C Clark, H. (2019). Cybersecurity Provisions and Trade Agreements. Harvard Business Law Review Online, 10, 1.

Kessler, O., C Werner, W. (2013). Expertise, uncertainty, and international law: a study of the Tallinn Manual on Cyberwarfare. Leiden Journal of International Law, 2c(4), 793-810.

Lehto, M. (2018). The modern strategies in the cyber warfare. Cyber Security: Power and Technology, 3-20.

Lupovici, A. (2016). The "attribution problem" and the social construction of "violence": taking cyber deterrence literature a step forward. International Studies Perspectives, 17(3), 322-342.

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., C Ni, W. (2018). Anatomy of threats to the internet of things. IEEE communications surveys & tutorials, 21(2), 1636-1675.

Mazanec, B. M. (2015). The evolution of cyber war: International norms for emerging-technology weapons. U of Nebraska Press.

Polyakova, A., C Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models. Policy brief, democracy and disorder series, 1-22.

Rid, T., C McBurney, P. (2012). Cyber-weapons. the RUSI Journal, 157(1), 6-13.

Robinson, M., Jones, K., C Janicke, H. (2015). Cyber warfare: Issues and challenges. Computers & security, 4S, 70-94.

Scarfone, K., Souppaya, M., Cody, A., C Orebaugh, A. (2008). Technical guide to information security testing and assessment. NIST Special Publication, 800(115), 2-25.

Shackelford, S. J., Richards, E. L., Raymond, A. H., C Craig, A. N. (2015). Using BITs to Protect Bytes: Promoting Cyber Peace by Safeguarding Trade Secrets Through Bilateral Investment Treaties. Am. Bus. LJ, 52, 1.

Uniacke, R. D. (2019). Dissuading Unrestricted Warfare: A Review on the Viability of Cyber Deterrence Strategies against the Chinese State Utica College].

Watney, M. (2014). Challenges pertaining to cyber war under international law. 2014 Third International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec),

Whyte, C. (2015). Power and predation in cyberspace. Strategic Studies Quarterly, S(1), 100-118.

Wing, K. T. (2004). Assessing the effectiveness of capacity-building initiatives: Seven issues for the field. Nonprofit and Voluntary Sector Quarterly, 33(1), 153-160.