Cyber, Disinformation and AI: Evolving Uses of ICT in Peace and Conflict

Working Group 9.10: ICT Uses in Peace and War

Brett van Niekerk(✉)

Durban University of Technology, Durban ZA, South Africa
brettv@dut.ac.za

Abstract. Working Group 9.10 is the newest group under Technical Committee 9, and it has a focus on ICT and its impact and uses in promoting and maintaining peace, as well as the use of ICTs in conflict and war. The focus of the working group's activities thus far has related to cybersecurity and cyberwarfare, with members being involved in organizing conference and specialist tracks, with other book projects and activities with related communities. After giving an introduction and history to the working group, the chapter covers some of the major themes and recent developments that are related to the themes of the working group.

Keywords: Autonomous Weapons · Critical Infrastructure Protection · Cyberwarfare · Cybersecurity · Online Advocacy

1 Overview

The aim of Working Group 9.10: ICT Uses in Peace and War is to provide a focused effort from multiple stakeholders to seek solutions to questions and areas of investigation in the primary field of study of the group. The group provides a platform to facilitate discussion, collaborative research, and development and presentation or publication of the research, lessons learnt, use cases, risk/impact assessments, and case studies [1].

The scope of the working group includes the effect, threats, and influences posed by ICTs at international, national, societal and individual levels, with particular relevance to activities of maintaining peace and during times of conflict. The scope also extends to how the various hierarchical levels of society perceive these threats, impacts and influences. Emerging from this, the following themes are considered core (although not exhaustive) to the working group, and are listed in alphabetical order:

- Artificial intelligence and machine learning in conflict and cyber security
- Autonomous weapons systems
- Cyber warfare
- Cyber security awareness
- Forensic applications and solutions
- Governance and standards

Published by Springer Nature Switzerland AG 2024
C. Leslie and D. Kreps (Eds.): *Current Directions in ICT and Society*, IFIP AICT 700, pp. 134–148, 2024.
https://doi.org/10.1007/978-3-031-50758-8_9

- Hacking, cracking, and other technical challenges
- ICT, critical infrastructure, and society
- ICT impacts on international relations and international security
- ICT strategies from a holistic, peaceful, and humane perspective
- ICT uses to prevent conflicts and contribute to peace
- ICT uses from a military perspective
- Legal, ethical, and social issues related to information security
- Promotion of democratic practices through ICT use
- Research and education on the impact of ICT in peace and war
- Social aspects of critical infrastructure protection
- Social networking
- Socio-technical aspects of ICT uses in peace and war
- Strategic information security
- Threat assessments
- Vulnerability assessments

The activities of the working group have included specialist tracks and round-table discussions at international conferences and collaborative research amongst its members.

2 History

Working Group 9.10 is the youngest of the working groups under Technical Committee 9 (TC 9), and was formally established in 2014 by Louise Leenen, with Leigh Armistead as vice-chair and Brett van Niekerk as secretary. At the beginning of 2020, Joey Jansen van Vuuren stepped in as vice-chair, Leigh Armistead moved to secretary, and Brett van Niekerk moved to chair the group. The working group has membership hailing from 18 countries.

The primary activities of the working group are specialist tracks at international conferences, such as the International Conference on Cyber Warfare and Security (ICCWS), the European Conference on Cyber Warfare and Security (ECCWS), and the IFIP TC 9 Human Choice in Computing (HCC). In 2015 and 2019, the working group chair was also co-chair of ICCWS. In 2020, the chair and vice-chair were co-editors for a special issue of the *Journal of Information Warfare* related to themes of the working group. There have also been numerous papers in journals and conferences that were collaboration amongst two or more members of the working group.

Other notable achievements from member of the working group include four making the Top 50 Women in Cybersecurity in Africa list in 2020 [2], and the chair and two members collaborating and winning the Global Cyberpeace Challenge policy and strategy track in 2021 [3].

3 Themes

Communications have played an important role in adverting crises and during conflict. The Allied effort to break the German and Japanese encryption during World War II and the implementation of a ‘hotline’ between Washington, D.C. and Moscow following the Cuban missile crisis illustrate this importance. The key theme in terms of current trends that is related to the working group relates to cybersecurity, and the increasing prevalence of cybersecurity in international security.

3.1 Cybersecurity and Cyber Operations in International Security

A Brief History of Major Cyber-Attacks. With the growing prevalence of computers and the Internet, it was not long before espionage and computer attacks were being seen. This section provides a summary, while not exhaustive, that illustrates the major trends of cyber-attacks in an international security context.

Initially, there was primarily espionage related activity, such as MOONLIGHT MAZE (1998) and TITAN RAIN (2003) [4, 5]. The first major disruptive attacks were denial-of-service attacks against Estonia (2007) and Georgia (2008) [6, 7]. The attacks against Georgia were of particular interest as they came prior to a physical military operation [7].

Whilst there was concern about the possibility of a cyber-attack against critical infrastructure which was driving research into cybersecurity, there was little to confirm these fears until the Stuxnet attack was uncovered in 2010, where the malware was used to target and damage centrifuges in Iran's nuclear enrichment facility. This particular attack is often cited as an example of the possibilities of cyber-warfare due to its relative sophistication and its ability to create physical damage by affecting industrial control systems [8, 9]. In December 2015, another cyber-attack attributed to state-baked actors (known and Sandworm) resulted in physical affects: in December 2015 the Ukrainian power grid experienced outages due to the BlackEnergy malware [10, 11].

Where Stuxnet and BlackEnergy targeted 'traditional' industrial controls systems, hyper-connectivity of devices, known as the Internet of Things (IoT) also began to pose security risks due to numerous insecure devices accessible over the Internet. The most notable incident was the Mirai botnet, which controlled compromised CCTV devices for the purposes of DDoS attacks. Two major attacks were attributed to Mirai botnets: in October 2016 the infrastructure and service provider Dyn was targeted, resulting in widespread outages of major social media and webpages in the U.S. [12]; and then against one of Liberia's major telecommunications organizations, effectively blocking the nation's Internet access [13].

In 2016, a group calling themselves the Shadow Brokers emerged, trying to auction cyber-attack tools, claimed to be stolen from a nation state. After the auction failed, the group leaked various tools online [14]. One of these, EternalBlue, was used in the two 2017 ransomware worm incidents: WannaCry and NotPetya, both of which were attributed to nation-states [15, 16]. These two incidents were of particular importance as they were the first ransomware variants with worm capability; they were also notable due to the disruption they wreaked on hospitals and major international organizations. During 2020, amidst the COVID-19 pandemic, ransomware again became consistent problem as they affected hospitals that were already burdened by the growing infections [17, 18]. Whilst these attacks were not attributed to state or state-backed actors, it illustrated how disruptive non-state actors could be when interfering with already constrained social systems. In addition to these attacks, there were reports of state of state-backed espionage targeting medical research, particularly those related to vaccine development [19].

In December 2020, reports began emerging of numerous organizations that had been affected by a cyber-attack; it was eventually discovered that a vendor providing network management solutions, SolarWinds, had been compromised, and the software updates deployed malware allowing the attackers to gain access to their targets [20]. This attack

is the best illustration of a supply-chain attack at the time of writing and is notable in the number of major technology and government departments that were compromised by the attack. A few months later, another major attack was discovered, exploiting a vulnerability in Microsoft Exchange servers. While organizations hurried to patch their systems, numerous hacking groups, including those associated with nation-states, were leveraging off the vulnerability to conduct espionage and data exfiltration [21].

In January 2022, Russian forces entered Ukraine in what was termed a 'special military operation'. There was an expectation of significant cyber-operations; however, initially there appeared to have been limited activity in the cyber domain. Details began emerging of the various cyber incidents related to the conflict, and a tracker by the CyberPeace Institute has recorded 918 cyber incidents as of 13 January 2023 – a year into the conflict [102].

Where this section gave an overview of cyber-attacks related to international security, there is also a diplomatic perspective. The next section discusses the international relations aspects to cyber-security.

Developments in Cyber Diplomacy and International Law. With the growing prevalence of activity on the Internet that has negatively impacts security, be it nation-state, criminal, or other actors, there have been attempts for the diplomatic and international law communities to respond to the growing threats. This section provides an overview of the efforts and studies that focus on these perspectives.

The first major attempt for international coherence was the Council of Europe's Convention on Cybercrime, more commonly known as the Budapest Convention. The focus was to provide a degree of consistency to the response to cybercrime, and also provide mechanisms for mutual assistance and collaboration amongst nations in their investigations into online criminal activity [22]. The African Union also established a Convention on Cybercrime and Personal Data Protection, known as the Malabo Convention [23].

While the Budapest and Malabo conventions focused on collaboration to mitigate cybercrime, gaps remained in how international law applies to cyber-operations, in particular those relating to conflict and human rights. Two in-depth academic studies, known as the Tallinn manuals, discuss a number of considerations in applying existing international law to cyber-warfare and cyber operations [24, 25].

At the United Nations, a series of Group of Government Experts (GGEs) were convened to consider "Developments in the Field of Information and Telecommunications in the Context of International Security" and then "Advancing responsible State behavior in cyberspace in the context of international security" [26]. There have been six completed GGEs from 2003 to 2021 [26]. The 2013 report confirmed the applicability of international law to cyber space, and the 2015 report proposed a series of norms of responsible state behavior in cyberspace [27, 28]. In addition to this, an Open Ended Working Group was convened, which was notable for its inclusivity through a multi-stakeholder approach, as well as achieving a consensus report in February 2021, with a second in progress from 2021–2025. There is also a proposed Program of Action that is considered an upcoming process at the time of writing [26].

Other processes and initiatives provide similar discussion, and often feed into the UN processes. For example, the Global Commission on the Stability of Cyberspace (GCSC) proposed a series of norms and definitions [29] as discussion and input to the

UN OEWG process. The Paris Call for trust and security in cyberspace is a multi-stakeholder initiative by the French government that has gained support from over 1000 entities, and advocates nine principles [30], which are similar in concept to the norms proposed by the GGE and GCSC. There are a number of other NGOs and initiatives that focus on related issues, such as The Geneva Dialogue on Responsible Behavior in Cyberspace [31], The Cybersecurity Tech Accord [32], Global Partners Digital [33], and the Global Forum on Cyber Expertise [34]. While this list is not exhaustive, it illustrates the recognition of the global importance of these issues. In addition to the norms and principles for good/responsible practice, these processes and initiatives also focused on confidence building measures and capacity building.

The norms and processes described in the preceding paragraphs are voluntary (i.e., non-binding), and a number of discussion around cybersecurity and international law are still open to interpretation. For instance, determining a use of force, act of war, or proportional responses in cyberspace is still uncertain. In practice, there has often been public attribution (usually denied by the alleged perpetrators) [15, 19] and sanctions against individuals implicated [35, 36]. An example of a retaliatory cyber-attack is a report that Israel targeted a major Iranian port in response to an alleged Iranian cyber-attack against an Israeli water system [37].

Key Works Related to Cybersecurity at National and International Levels. A number of selected works related to cybersecurity are presented below in alphabetical order of the title.

Books:

- *@War* by Shane Harris [38]
- *Countdown to Zero Day* by Kim Zetter [9]
- *The Cybersecurity Dilemma* by Ben Buchanan [39]
- *Cyberwar and Information Warfare*, edited by Daniel Ventre [40]
- *Cyber Conflict: Competing National Perspectives*, edited by Daniel Ventre [41]
- *Cyber Espionage and International Law* by Russel Buchan [42]
- *Cyber Mercenaries* by Tim Maurer [43]
- *Cyber Operations and International Law* by François Delerue [44]
- *Cyber Persistence Theory* by Michael Fischerkeller, Emily Goldman, Richard Harknett [106]
- *Cyber Strategy* by Valeriano, Jensen and Maness [45]
- *Cyber War versus Cyber Realities* by Brandon Valeriano and Ryan C. Maness [46]
- *Cyber War: The Next Threat to National Security and What to Do About It* by Richard A. Clarke and Robert K. Knake [47]
- *Dark Territory* by Fred Kaplan [48]
- *Global Information Warfare* by Andrew Jones and Gerald L. Kovacich [49]
- *The Hacked World Order* by Adam Segal [50]
- *The Hacker and the State* by Ben Buchanan [51]
- *Information Operations Matters* by Leigh Armistead [52]
- *Information Operations: Warfare and the Hard Realities of Soft Power,* edited by Leigh Armistead [53]
- *Information Warfare*, 2nd ed., by Daniel Ventre [54]

- *Information Warfare: Separating Hype from Reality*, edited by Leigh Armistead [55]
- *Information Warfare in the Age of Cyber Operations* by Christopher Whyte, Trevor Thrall, and Brian Mazanec [109]
- *Inside Cyber Warfare* by Jeffrey Carr [56]
- *Modelling Nation-state Information Warfare and Cyber-operations*, edited by Brett van Niekerk, Trishana Ramluckan, and Neal Kushwaha [103]
- *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* by Max Smeets [104]
- *Offensive Cyber Operations* by Daniel Moore [105]
- *Russian Information Warfare* by Bilyana Lilly [107]
- *The Tallinn Manual and The Tallinn Manual 2.0*, edited by Michael Schmitt [24, 25]
- *The Virtual Battlefield* by Christian Czosseck and Kenneth Geers [57]

Conferences and journals:

- European Conference on Cyber Warfare and Security (https://www.academic-conferences.org/conferences/eccws/)
- International Conference on Cyber Conflict (https://www.cycon.org/)
- International Conference on Cyber Warfare and Security (https://www.academic-conferences.org/conferences/iccws/)
- International Journal of Cyber Warfare and Terrorism (https://www.igi-global.com/journal/international-journal-cyber-warfare-terrorism/1167)
- Journal of Information Warfare (https://www.jinfowar.com), with a special issue on Ukraine [117] edited by Bill Hutchinson
- Journal of Law & Cyber Warfare (https://www.jlcw.org/)

Other resources:

- CyberPeace Institute portal on cyber incidents during the Ukraine conflict [102]
- EU Cyber Direct Cyber Diplomacy Atlas [110]
- Geneva Internet Platform Digital Watch Portal [26]
- The Hague Centre for Strategic Studies Cyber Arms Watch [111]
- United Nations Institute for Disarmament Research Cyber Policy Portal [112]

3.2 Online Influence Operations and Activism

An Overview of the Theme. The growth of ICTs gave civil society, NGOs, and activists a greater voice. The first notable occurrence was the Zapatista movement, which changed from an insurgency to an online movement in 1994 [58]. Later occurrences saw mobile devices and social media begin playing a role in anti-government protests and similar movements. Initially, the use of such technology occurred in Iran, Moldova, Urumqi (in China) and Mozambique [59, 60]. Subsequently, social media activity was also apparent in documenting a military intervention in Zimbabwe, as well as supporting subsequent protests [61].

The two most notable examples are the Arab Spring events and in Ukraine. In 2010 mass government protests supported by the use of social media spread across North Africa and the Middle East, resulting in changes of government [62]. In the Ukraine, the scenario was more complex; initially, pro-EU protestors ousted a pro-Russia government; in these protests social media was used for communication, but also specifically arranging legal, medical, and other supplies for the protestors [62]. Following this, pro-Russian protests, supported by media and other influence operations began opposing the interim pro-EU government. Ultimately, the situation led to the annexation of the Crimea and a conflict in the Eastern Ukraine; this provides a good example of hybrid warfare, where media influence and cyber-attacks were effectively used as a pre-cursor to military actions [62].

Activism and influence operations can be related to information and cyber-security. An interpreter at the UK's General Communications Headquarters (GCHQ) leaked information on how the U.S. intended to spy on UN members prior to a vote on sending troops to Iraq [63], and a contractor for U.S. intelligence agencies leaked sensitive National Security Agency information [64]. WikiLeaks published numerous communications and documents from the military operations in Afghanistan and Iraq, as well as U.S. diplomatic communications, leaked by an intelligence analyst [65]. All of these major leaks were the result of internal actors breaching security; and these leaks have provided insights into the secret activities of governments' intelligence and cyber-operations.

WikiLeaks also released information obtained through cyber-attacks, such as from Sony Pictures, and emails from the Democrat's 2016 presidential campaign [65]. This latter incident is often associated with concerns of a broader influence operation to influence the elections, where messages across a broad range of social media was reportedly used to create divisions in the U.S. [66]. A PR firm, Cambridge Analytica, was embroiled in a scandal based on their messaging to influence voters based on data gathered about them on social media [67]; prior to this, Bell Pottinger was exposed using cynical and malicious messaging in South Africa, ultimately resulting in the collapse of the company [68].

During the COVID-19 pandemic in 2020, there were various attempts at disinformation and influence. Some disinformation campaigns were attributed to nations, particularly surrounding the origins of the virus [69]. Other nations used social media as a propaganda mechanism, targeting countries in an attempt to improve their image in conjunction to providing aid to those countries [70]. A disturbing trend was a handful of world leaders to also providing disinformation [71, 72].

The response to disinformation and influence operations has not yet achieved the growth that has been see for cyber-security. The Carnegie Endowment for International Peace hosts a Partnership for Countering Influence Operations [73]; this group is a partner to the Disinfodex, an online database of information about known disinformation operations [74]. Large tech firms also release dataset, such as Twitter's data on information operations [75]. National responses to disinformation, especially during the pandemic, was to pressure social media companies to enhance their efforts [76], or to outlaw disinformation and misinformation, which raised some debate due to concerns over restrictions on freedom of speech [77].

Key Works and Resources Related to Influence Operations, Disinformation and Online Activism. A number of selected works related to cybersecurity are presented below in alphabetical order based on the title.

- *Active Measures* by Thomas Rid [78]
- *Atlantic Council's Digital Sherlocks programme and 360/OS conference* [113, 114]
- Carnegie Endowment for International Peace Partnership for Countering Influence Operations [73]
- *Influence and Escalation* by Rebecca Hersman, Eric Brewer, Lindsey Sheppard, and Maxwell Simon [108]
- *Information Wars* by Richard Stengel [79]
- Special Issue on Countering Influence Operations, *Journal of Information Warfare*, edited by Alicia Wanless and James Pamment [80]
- *This Is not Propaganda* by Peter Pomerantsev [81]
- *The World Information War*, edited by Timothy Clack and Robert Johnson [82]
- *Towards Responsible AI in Defence: A Mapping and Comparative Analysis of AI Principles Adopted by States* by Alisha Anand and Harry Deng [116]

3.3 Artificial Intelligence, Autonomous Systems, and Surveillance

An Overview of the Current Issues within the Theme. With the increase of 'smart' or 'intelligent' systems that are connected, there are a number of concerns raised. In terms of commercially available devices, concerns usually revolve around privacy and the extent of information these devices and the manufacturers collect; this applies both to home automation and mobile devices [83]. When similar technological concepts are extended to physical security applications, such as facial recognition in CCTV surveillance, both privacy and accuracy become problematic. As surveillance systems are not in an 'ideal' environment there is the likelihood for incorrect matches; this becomes particularly problematic when incorrect matches are used as evidence for criminal or other legal proceedings [84, 85].

When such technology is employed in military and intelligence contexts, there are concerns that autonomous and semi-autonomous systems can potentially attack incorrect targets [86]. A fully autonomous system is defined as one that can perform target identification and selection, as well as attacking the target, with no human control [86]. As can be seen from the list of key works below, the majority of research and focus on this topic revolves around the ethics and law of using artificial intelligence and autonomous systems.

Key works and resources related to AI, autonomous systems, and surveillance. A number of selected works related to cybersecurity are presented below in alphabetical order based on the title.

- *Army of None* by Paul Scharre [87]
- *Autonomous Weapons Systems: Law, Ethics, Policy*, edited by Bhuta, Beck, Geiβ, Liu, Kreβ [88]
- *Autonomous Weapon Systems and the Law of Armed Conflict* by Tim McFarland [89]

- *Genius Weapons* by Louis A. Del Monte [90]
- *Killer Robots* by Armin Krishnan [91]
- *Killer Robots* by U.C. Jha [92]
- *Lethal Autonomous Weapons*, edited by Galliott, MacIntosh, and Ohlin [93]
- Organization for Economic Co-operation and Development (OECD) AI Policy Observatory [115]
- *Wired for War* by P.W. Singer [94]

4 Future Directions

The themes relevant to the working group have numerous possible future directions. This section will provide an overview of current and future events that are likely to drive the issues and research considered by the working group.

From a technical cyber security perspective, research in current and future attack trends [95], vulnerabilities, as well as improving detective and preventative controls will continue as future research avenues. As the Fourth Industrial Revolution continues and more technological innovations are introduced (such as 5G and quantum computing), the interactions between cyber security and the other pillars of 4IR will continue to evolve and require research [96]. There are already indications that the 4IR is evolving to the Fifth Industrial Revolution, which will increase the security challenges [97, 98]. In addition to the cyber-security perspective, the application of emerging technologies in conflict, peace, and security settings will require investigation, including the ongoing legal and ethical debate on autonomous weapons systems.

From the cyber diplomacy perspective, there are a number of initiatives at the time of writing: The UN Human Rights Office of the High Commissioner is developing a report on cyber mercenaries [99]; the mandate for the OEWG was extended for 2021–2025, with the GGE scheduled to completed in 2021 [26]; the next phase of the Paris Call is continuing in 2021 with a series of working groups [100]; and a second additional protocol for the Budapest Convention is in the consultation phase [101]. The number of initiatives in this area indicate that there will continue to be significant research and investigations continuing for the foreseeable future.

As disinformation and influence operations continue, there is likely to be ongoing discussion and an increasing number of forums considering disinformation and influence. There is also likely to be research aligning the detection and mitigation of influence operations with existing cyber security techniques. As with cyber security, emerging technologies are likely to increase the sophistication and reach of influence operations.

References

1. Working Group 9.10 – ICT Uses in Peace and War, IFIP TC 9. http://ifiptc9.org/9-10/
2. Ongeri, L.: Cyber in Africa has announced top 50 women in cybersecurity Africa finalists. https://www.ifree.co.ke/2020/07/cyber-in-africa-has-announced-top-50-women-in-cybersecurity-africa-finalists/. Accessed 21 Apr 2021
3. IFIP News.: IFIP WG 9.10 members win international cyber security competition. https://www.ifipnews.org/ifip-wg-9-10-members-win-international-cyber-security-competition/. Accessed 21 Apr 2021

4. Doman, C.: The first cyber espionage attacks: how operation Moonlight Maze made history. https://medium.com/@chris_doman/the-first-sophistiated-cyber-attacks-how-operation-moonlight-maze-made-history-2adb12cc43f7. Accessed 21 Apr 2021
5. Espiner, T.: Security experts lift lid on Chinese hack attacks, ZDNet. Archived from the original. https://web.archive.org/web/20061211145201/http://news.zdnet.com/2100-1009_22-5969516.html. Accessed 21 Apr 2021
6. McGuinness, D.: How a cyber attack transformed Estonia, BBC News. https://www.bbc.com/news/39655415. Accessed 21 Apr 2021
7. Markoff, J.: Before the gunfire, cyberattacks, The New York Times. https://www.nytimes.com/2008/08/13/technology/13cyber.html. Accessed 21 Apr 2021
8. Zetter, K.: An unprecedented look at Stuxnet, the world's first digital weapon, Wired. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/. Accessed 23 Apr 2021
9. Zetter, K.: Countdown to Zero Day. Crown Publishers, New York (2014)
10. Hultquist, J.: Sandworm Team and the Ukrainian Power Authority attacks, FireEye. https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html. Accessed 23 Apr 2021
11. Assante, M.: Confirmation of a coordinated attack on the Ukrainian power grid, SANS Institute. https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/. Accessed 23 Apr 2021
12. Fruhlinger, J.: The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet, CSO Online. https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html. Accessed 23 Apr 2021
13. Kirk, J.: UK sentences man for Mirai DDoS attacks against Liberia, BankInfoSecurity. https://www.bankinfosecurity.com/uk-sentenced-man-for-mirai-ddos-attacks-against-liberia-a-11933. Accessed 23 Apr 2021
14. Goodin, D.: Confirmed: hacking tool leak came from "omnipotent" NSA-tied group, ARS Technica. https://arstechnica.com/information-technology/2016/08/code-dumped-online-came-from-omnipotent-nsa-tied-hacking-group/. Accessed 23 Apr 2021
15. BBC News: Cyber-attack: US and UK blame North Korea for WannaCry. https://www.bbc.com/news/world-us-canada-42407488. Accessed 23 Apr 2021
16. Radio Free Europe: Ukraine Security Service blames Russia for recent cyberattack. https://www.rferl.org/a/cyberattack-ukraine-blames-russia/28589606.html. Accessed 23 Apr 2021
17. Cimpanu, C.: Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak, Zero Day. https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/. Accessed 23 Apr 2021
18. Osborne, C.: Major European private hospital operator struck by ransomware, Zero Day. https://www.zdnet.com/article/europes-largest-private-hospital-chain-struck-by-ransomware-attack/. Accessed 23 Apr 2021
19. Cimpanu, C.: US formally accuses China of hacking US entities working on COVID-19 research, Zero Day. https://www.zdnet.com/article/us-formally-accuses-china-of-hacking-us-entities-working-on-covid-19-research/. Accessed 23 Apr 2021
20. Scroxton, A.: SolarWinds cyber attack is 'grave risk' to global security, Computer Weekly. https://www.computerweekly.com/news/252493862/SolarWinds-cyber-attack-is-grave-risk-to-global-security. Accessed 18 Dec 2020
21. Baksh, M.: CISA, FBI link Exploitation of Microsoft Exchange to nation-state actors, NextGov. https://www.nextgov.com/cybersecurity/2021/03/cisa-fbi-link-exploitation-microsoft-exchange-nation-state-actors/172614/. Accessed 12 Mar 2021
22. Council of Europe: Budapest Convention and related standards. https://www.coe.int/en/web/cybercrime/the-budapest-convention. Accessed 27 Apr 2021

23. African Union: Convention on Cyber Security and Personal Data Protection, 2014. https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf. Accessed 11 Jul 2019
24. Schmitt, M.N.: Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, Cambridge (2013)
25. Schmitt, M.N.: Tallinn Manual 2.0: On The International Law Applicable to Cyber Operations. Cambridge University Press, Cambridge (2017)
26. Geneva Internet Platform: UN GGE and OEWG, Digital Watch. https://dig.watch/processes/un-gge. Accessed 27 Jan 2023
27. United Nations General Assembly: Resolution adopted by the General Assembly on 27 December 2013, 68/243. Developments in the field of information and telecommunications in the context of international security. https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/243. Accessed 27 Apr 2021
28. United Nations General Assembly: Resolution adopted by the General Assembly on 23 December 2015, 70/237. Developments in the field of information and telecommunications in the context of international security. https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2016/01/A-RES-70-237-Information-Security.pdf. Accessed 27 Apr 2021
29. Global Commission on the Stability of Cyberspace. Advancing Cyberstability Final Report. https://cyberstability.org/report/. Accessed 27 Apr 2021
30. The Paris Call for Trust and Security in Cyberspace. https://pariscall.international/en/. Accessed 27 Apr 2021
31. The Geneva Dialogue on Responsible Behavior in Cyberspace. https://genevadialogue.ch/. Accessed 27 Apr 2021
32. The Cybersecurity Tech Accord. https://cybertechaccord.org/about/. Accessed 27 Apr 2021
33. Global Partners Digital. https://www.gp-digital.org/. Accessed 27 Apr 2021
34. Global Forum on Cyber Expertise. https://thegfce.org/. Accessed 27 Apr 2021
35. Council of the European Union.: EU imposes the first ever sanctions against cyber-attacks. https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/. Accessed 27 April 2021
36. Scroxton, A.: Biden sanctions Russia over SolarWinds cyber attacks, Computer Weekly. https://www.computerweekly.com/news/252499384/Biden-sanctions-Russia-over-SolarWinds-cyber-attacks. Accessed 27 Apr 2021
37. TOI Staff: Israel behind cyberattack that caused 'total disarray' at Iran port – report, Times of Israel. https://www.timesofisrael.com/israel-said-behind-cyberattack-that-caused-total-disarray-at-iran-port-report/. Accessed 27 Apr 2021
38. Harris, S.: @War: The Rise of the Military-Internet Complex. Eamon Dolan, Boston (2014)
39. Buchanan, B.: The Cybersecurity Dilemma. Oxford University Press, Oxford (2016)
40. Ventre, D.: (ed.): Cyberwar and Information Warfare. ISTE and Wiley, London and Hoboken, NJ. (2011)
41. Ventre, D.: (ed.): Cyber Conflict: Competing National Perspectives. ISTE and Wiley, London and Hoboken, NJ. (2012)
42. Buchan, R.: Cyber Espionage and International Law. Bloomsbury, Oxford (2019)
43. Maurer, T.: Cyber Mercenaries. Cambridge University Press, Cambridge (2018)
44. Delerue, F.: Cyber Operations and International Law. Cambridge University Press, Cambridge (2020)
45. Valeriano, B., Jensen, B., Maness, R.C.: Cyber Strategy: The Evolving Character of Power and Coercion. Oxford University Press, Oxford (2018)
46. Valeriano, B., Maness, R.C.: Cyber War versus Cyber Realities. Oxford University Press, Oxford (2015)

47. Clarke, R.A., Knake, R.A.: Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins, New York (2010)
48. Kaplan, F.: Dark Territory: The Secret History of Cyber War. Simon & Schuster, New York (2016)
49. Jones, A., Kovacich, G.L.: Global Information Warfare: The New Digital Battlefield, 2nd edn. CRC Press, Boca Raton, FL (2016)
50. Segal, A.: The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. Hachette, New York (2016)
51. Buchanan, B.: The Hacker and the State. Harvard University Press, Cambridge, Ma (2020)
52. Armistead, E.L.: Information Operations Matters: Best Practices. Potomac Books, Washington, D.C. (2010)
53. Armistead, E.L. (ed.): Information Operations: Warfare and the Hard Realities of Soft Power. Potomac Books, Washington, D.C. (2004)
54. Ventre, D.: Information Warfare, 2nd ed. ISTE and Wiley, London and Hoboken, NJ. (2016)
55. Armistead, E.L. (ed.): Information Warfare: Separating Hype from Reality. Potomac Books, Washington, D.C. (2007)
56. Carr, J.: Inside Cyber Warfare: Mapping the Cyber Underworld. O'Reilly Media, Sebastopol, CA (2010)
57. Czosseck, C., Geers, K.: The Virtual Battlefield: Perspectives on Cyber Warfare. IOS Press, Amsterdam (2009)
58. Morello, H.J.: E-(re)volution: Zapatistas and the emancipatory Internet. Contra Corriente: J. Soc. Lit. Lat. Am. **4**(2), 54–76 (2007)
59. World Movement for Democracy: Case Study on Twitter. http://www.wmd.org/resources/whats-being-done/information-and-communication-technologies/casestudy-twitter. Accessed 17 Jun 2010
60. News24.: Mozambique unrest shows power of SMSes. https://www.news24.com/news24/moz-unrest-shows-power-of-smses-20100907. Accessed 27 Apr 2021
61. van Niekerk, B., De Barros, M.J.Z., Ramluckan, T.: An analysis of Twitter during the 2017 Zimbabwean military intervention. In: Kreps, D., Komukai, T., Gopal, T.V., Ishii, K. (eds.) 14th IFIP TC 9 International Conference on Human Choice and Computers, HCC14 2020, pp. 233–247. Springer, Heidelberg (2020)
62. van Niekerk, B.: Information warfare in the 2013–2014 Ukraine crisis. In: Richet, J.L. (ed.), Cybersecurity Policies and Strategies for Cyberwarfare Prevention, pp. 311–342. IGI Global, Hershey, PA (2015)
63. Bright, M.: Katharine Gun: Ten years on what happened to the woman who revealed dirty tricks on the UN Iraq war vote? The Guardian. https://www.theguardian.com/world/2013/mar/03/katharine-gun-iraq-war-whistleblower. Accessed 27 Apr 2021
64. MacAskill, E.: Interview with Snowden, The Guardian. https://www.theguardian.com/us-news/ng-interactive/2019/sep/13/edward-snowden-interview-whistleblowing-russia-ai-permanent-record. Accessed 27 Apr 2021
65. BBC News: Wikileaks: document dumps that shook the world. https://www.bbc.com/news/technology-47907890. Accessed 27 Apr 2021
66. Hosenball, M.: Russia used social media for widespread meddling in U.S. politics: reports, Reuters. https://www.reuters.com/article/us-usa-trump-russia-socialmedia-idUSKBN1OG257. Accessed 27 Apr 2021
67. Confessore, N.: Cambridge Analytica and Facebook: the scandal and the fallout so far, The New York Times. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Accessed 27 Apr 2021
68. Cave, A.: Deal that undid Bell Pottinger: inside story of the South Africa scandal, The Guardian. https://www.theguardian.com/media/2017/sep/05/bell-pottingersouth-africa-pr-firm. Accessed 27 Apr 2021

69. Swan, B.W.: State report: Russian, Chinese and Iranian disinformation narratives echo one another, Politico. https://www.politico.com/news/2020/04/21/russia-china-iran-disinformation-coronavirus-state-department-193107. Accessed 27 Apr 2021
70. Kao, J., and Li, M.S.: How China built a Twitter propaganda machine then let it loose on Coronavirus, ProPublica. https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus. Accessed 27 Apr 2021
71. Friedman, U.: The Coronavirus-denial movement now has a leader, The Atlantic. https://www.theatlantic.com/politics/archive/2020/03/bolsonaro-coronavirus-denial-brazil-trump/608926/. Accessed 27 Apr 2021
72. McCarthy, T.: 'It will disappear': the disinformation Trump spread about the coronavirus – timeline, The Guardian. https://www.theguardian.com/us-news/2020/apr/14/trump-coronavirus-alerts-disinformation-timeline. Accessed 27 Apr 2021
73. Carnegie Endowment for International Peace.: Partnership for Countering Influence Operations. https://carnegieendowment.org/specialprojects/counteringinfluenceoperations. Accessed 27 Apr 2021
74. Disinfodex: https://disinfodex.org/. Accessed 27 Apr 2021
75. Twitter Transparency.: Information operations. https://transparency.twitter.com/en/reports/information-operations.html. Accessed 27 Apr 2021
76. Skelton, S.K.: Government tells social media companies they must go further to address disinformation, Computer Weekly. https://www.computerweekly.com/news/252483063/Government-tells-social-media-companies-they-must-do-more-to-address-disinformation. Accessed 27 Apr 2021
77. Hodgson, T.F., Farise, K., and Mavedzenge, J.: Southern Africa has cracked down on fake news, but may have gone too far, Mail and Guardian. https://mg.co.za/analysis/2020-04-05-southern-africa-has-cracked-down-on-fake-news-but-may-have-gone-too-far/. Accessed 27 Apr 2021
78. Rid, T.: Active Measures: The Secret History of Disinformation and Political Warfare. Profile Books, London (2020)
79. Stengel, R.: Information Wars: How We Lost the Global Battle against Disinformation and What We Can Do About It. Atlantic Books, London (2019)
80. Wanless, A., Pamment, J., eds.: Special issue on countering influence operations. J. Inf. Warfare **18**(3) (2019)
81. Pomerantsev, P.: This is not Propaganda: Adventures in the War Against Reality. Faber & Faber, London (2019)
82. Clack, T., Johnson, R.: The World Information War: Western Resilience, Campaigning, and Cognitive Effects. Routledge, New York (2021)
83. PYMNTS.: EU probe into IoT targets Siri, Alexa over data collection. https://www.pymnts.com/news/regulation/2020/eu-probe-into-iot-targets-siri-alexa-over-data-collection/. Accessed 28 Apr 2021
84. Allen, K.: Future of facial recognition technology in Africa, Institute for Security Studies. https://issafrica.org/iss-today/future-of-facial-recognition-technology-in-africa. Accessed 28 Apr 2021
85. Hill, K.: Wrongfully accused by an algorithm, The New York Times. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html. Accessed 28 Apr 2021
86. Future of Life Institute: Lethal autonomous weapons systems. https://futureoflife.org/lethal-autonomous-weapons-systems/. Accessed 28 Apr 2021
87. Scharre, P.: Army of None: Autonomous Weapons and the Future of War. W.W. Norton & Company, New York (2019)
88. Bhuta, N., Beck, S., Geiβ, R., Liu, H., Kreβ, C. (eds.): Autonomous Weapons Systems: Law, Ethics. Policy. Cambridge University Press, Cambridge (2016)

89. McFarland, T.: Autonomous Weapon Systems and the Law of Armed Conflict. Cambridge University Press, Cambridge (2020)
90. Del Monte, L.A.: Genius Weapons: Artificial Intelligence, Autonomous Weaponry, and the Future Warfare. Prometheus Books, New York (2018)
91. Krishnan, A.: Killer Robots: Legality and Ethicality of Autonomous Weapons. Routledge, New York (2009)
92. Jha, U.C.: Killer Robots: Lethal Autonomous Weapon Systems Legal. Ethical and Moral Challenges. Vij Books India, Delhi (2016)
93. Galliott, J., MacIntosh, D., Ohlin, J.D. (eds.): Lethal Autonomous Weapons: Re-Examining the Law and Ethics of Robotic Warfare. Oxford University Press, Oxford (2021)
94. Singer, P.W.: Wired for War: The Robotics Revolution and Conflict in the 21st Century. Penguin Press, London (2009)
95. Greenberg, I.: Fifth-generation cyberattacks are here. How can the IT industry adapt? World Economic Forum. https://www.weforum.org/agenda/2021/02/fifth-generation-cyberattacks/. Accessed 29 Apr 2021
96. Coulehan, G.: The Fourth Industrial Revolution – AI, Quantum, and IoT Impacts on Cybersecurity, Security Boulevard. https://securityboulevard.com/2021/02/the-fourth-industrial-revolution-ai-quantum-and-iot-impacts-on-cybersecurity/. Accessed 29 Apr 2021
97. Naidoo, V.: The fifth industrial revolution looms, ITWeb. https://www.itweb.co.za/content/WnxpE74D2jg7V8XL. Accessed 29 Apr 2021
98. Djekic, M.D.: The perspectives of the 5th Industrial Revolution, Cyber Defense Magazine. https://www.cyberdefensemagazine.com/the-perspectives/. Accessed 29 Apr 2021
99. UN Human Rights Office of the High Commissioner: Call for inputs: report on the provision of military and security cyber products and services by 'cyber mercenaries' and its human rights impact. https://www.ohchr.org/EN/Issues/Mercenaries/WGMercenaries/Pages/Report-Cyber-Mercenaries-2021.aspx. Accessed 29 Apr 2021
100. France Diplomacy: Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace. https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in. Accessed 29 Apr 2021
101. Council of Europe: Consultations with civil society, data protection authorities and industry on the 2nd Additional Protocol to the Budapest Convention on Cybercrime. https://www.coe.int/en/web/cybercrime/protocol-consultations. Accessed 29 Apr 2021
102. CyberPeace Institute: Cyber Threats. https://cyberconflicts.cyberpeaceinstitute.org/threats. Accessed 27 Jan 2023
103. van Niekerk, B., Ramluckan, T., Kushwaha, N. (eds.): Modelling Nation-state Information Warfare and Cyber-operations. Academic Conferences and Publishing International, Reading, UK (2022)
104. Smeets, M.: No Shortcuts: Why States Struggle to Develop a Military Cyber-Force. Hurst, London (2022)
105. Moore, D.: Offensive Cyber Operations. Hurst, London (2022)
106. Fischerkeller, M.P., Goldman, E.O., Harknett, R.J.: Cyber Persistence Theory. Oxford University Press, New York (2002)
107. Lilly, B.: Russian Information Warfare. Naval Institute Press, Annapolis, MD (2022)
108. Hersman, R., Brewer, E., Sheppard, L., Simon, M.: Influence and Escalation: Implications of Russian and Chinese Influence Operations for Crisis Management. Center for Strategic and International Studies. https://www.csis.org/analysis/influence-and-escalation-implications-russian-and-chinese-influence-operations-crisis. Accessed 27 Jan 2023
109. Whyte, C., Thrall, A.T., Mazanec, B.M.: Information Warfare in the Age of Cyber Conflict. Routledge, Milton Park, UK (2021)

110. EU Cyber Direct.: Cyber Diplomacy Atlas. https://eucyberdirect.eu/atlas. Accessed 14 Feb 2023
111. The Hague Centre for Strategic Studies.: Cyber Arms Watch. https://hcss.nl/cyber-arms-watch/. Accessed 14 Feb 2023
112. United Nations Institute for Disarmament Research.: Cyber Policy Portal. https://cyberpolicyportal.org/. Accessed 14 Feb 2023
113. Atlantic Council.: Digital Sherlocks. https://www.digitalsherlocks.org/. Accessed 14 Feb 2023
114. Atlantic Council.: 360/OS. https://www.digitalsherlocks.org/360-os. Accessed 14 Feb 2023
115. Organization for Economic Co-operation and Development (OECD).: AI Policy Observatory. Accessed 14 Feb 2023
116. Anand, A., and Deng, H.: Towards Responsible AI in Defence: A Mapping and Comparative Analysis of AI Principles Adopted by States, United Nations Institute for Disarmament Research: Geneva (2023). https://unidir.org/publication/towards-responsible-ai-defence-mapping-and-comparative-analysis-ai-principles-adopted
117. Hutchinson, W. (ed.) Special Issue on Ukraine. J. Inf. Warfare **22**(1) (2023)