

Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

Digital Threats in Modern Armed Conflicts

Brahimi Smail^{*},

Lounisi Ali University Blida2(Algeria), smailbrahimi405@gmail.com

Date of send: 01 / 06 / 2024

date of acceptance: 01 / 08 /2024

Date of Publication: 01/09/2024

^{*}Corresponding author

Abstract :

Modern armed conflicts are increasingly involving cyberspace, as both states and non-state actors use it to achieve their goals and gain strategic benefits. However, this has also brought new challenges, such as disinformation campaigns and cyberattacks aiming to sway public opinion and infrastructure. Understanding cyber threats in armed conflicts is crucial for developing effective protection tactics and reducing damage. Cyberwarfare, unlike conventional warfare, deals with information, manipulation, and disruption, often contradicting established military doctrines and state behavior standards.

Keywords: digital ; threats ; cyber attacks ; armed conflicts

Introduction

The battleground in modern armed conflicts is much larger than the conventional theaters of war. As a result of the widespread use of digital technology, both states and non-state actors have taken advantage of cyberspace to further their goals, displace enemies, and obtain strategic benefits. But this change has also brought with it a host of new difficulties, such as disinformation campaigns spreading and cyberattacks aiming at swaying public opinion and key infrastructure. It is vital to comprehend the terrain of cyber threats in armed conflicts in order to formulate efficacious protection tactics and alleviate any damage.

The ubiquitous menace of digital violence is a new and frightening specter in the field of modern warfare. Cyberspace has become more important as states and non-state entities use digital technology more and more.

The spread of digital technologies has revolutionized state power projection, strategic goal pursuit, and adversarial relations. The range of digital dangers in modern warfare is wide and diverse, ranging from sophisticated cyber espionage campaigns aimed at sensitive government networks to disruptive assaults intended to destroy vital infrastructure. Furthermore, because of the interconnectivity of the world's networks and the growing dependence of society on information and communication technologies (ICTs), countries are now at risk from hostile cyberattacks that might have devastating effects.

The advent of cyberwarfare as a unique facet of contemporary warfare carries significant ramifications for international relations, warfare tactics, and national security. In contrast to conventional warfare, which focuses mostly on the physical destruction of targets, cyberwarfare deals with information, manipulation, and disruption. Because of this, the instruments and strategies used in cyberspace frequently contradict established military doctrines and standards of state behavior.

Therefore, what do we mean by digital threats in armed conflicts, what are their forms and risks in such conflicts, and what is the position and role of international humanitarian law towards them?

THE FIRST TOPIC : Cyber Attacks: A Lethal Weapon of Modern Warfare

First requirement: Definition of cyber Attacks

Cyberattacks are intentional acts that target the availability, confidentiality, or integrity of computer systems, networks, or data. They frequently try to cause damage, interrupt operations, or obtain unauthorized access to private data. Within the framework of contemporary warfare, cyberattacks constitute a powerful and pervasive kind of aggression that can seriously harm civilian populations, military installations, and vital services.⁽¹⁾

Second requirement: The danger of cyber attacks

Cyberattacks are now a potent tool in the toolboxes of both state actors and cybercriminals. The 2010 discovery of the infamous Stuxnet malware serves as an example of how cyberattacks may physically demolish industrial control systems, particularly those involved in Iran's nuclear program ⁽²⁾

Stuxnet. It is generally accepted to have been developed jointly by the US and Israel with the intention of undermining Iran's nuclear program by focusing on the industrial control systems (ICS) that are employed in its uranium enrichment facilities, especially the nuclear plant in Natanz.

Siemens Step7 software, which is frequently used to regulate industrial operations, particularly those involved in uranium enrichment, was the explicit target of the Stuxnet worm. Once inside a system, Stuxnet would propagate by way of local area networks and USB flash drives, looking for particular configurations that coincided with those seen in the Natanz plant. Next, it changed the centrifuges' programmable logic controllers (PLCs), making them run at speeds that would harm the machinery. ⁽³⁾

These kinds of attacks highlight how susceptible vital infrastructure is to cyberattacks, with potentially disastrous results that might affect everything from military operations to large-scale power outages.

Furthermore, government institutions and defense contractors have been the target of state-sponsored hacking groups more and more. Famous instances are Fancy Bear from Russia and APT10 from China, both of which have been connected to cyberattacks intended to steal confidential data and interfere with the activities of opponents ⁽⁴⁾. These actions demonstrate how the distinction between cyberwarfare and conventional warfare is becoming increasingly hazy, with the

combat extending beyond physical borders into the interconnected networks of the digital world.

THE SECOND TOPIC: Information Warfare: Weaponizing Disinformation

First requirement: The Importance of Information Warfare

The deliberate use of information and communication technologies to alter behavior, shape perceptions, and further ideological, military, or political goals is known as information warfare. The weaponization of disinformation, or the purposeful spread of false or misleading information to mislead, disrupt, or undermine adversaries, is central to the idea of information warfare. ⁽⁵⁾

Second requirement: information warfare as powerful instrument

These days, information warfare is a powerful instrument for rewriting history, swaying public opinion, and causing strife between enemies. Disinformation campaigns can threaten democratic processes and destabilize countries, as demonstrated by the Russian government's intervention in the 2016 U.S. presidential election. ⁽⁶⁾ Foreign players attempted to take advantage of preexisting differences and instill mistrust in democratic institutions through the manipulation of social media, cyber operations, and the propagation of false narratives.

Similarly, information has been weaponized to further strategic goals in wars like the current crisis between Russia and Ukraine. Propaganda campaigns have been launched by both sides in an effort to skew reality and give themselves a psychological advantage over their opponents ⁽⁷⁾ Controlling the narrative has become essential to modern warfare in an era where information is instantly shared across international networks.

THE THIRD TOPIC: Technological Vulnerabilities: Unforeseen Risks in the Digital Age

First requirement: Technological Vulnerabilities as Advantage to Cause Harm

Technological vulnerabilities are flaws or vulnerabilities in technological infrastructures or systems that can be used to alter, interfere with, or compromise their operation. These weaknesses can provide serious dangers in armed conflicts

because adversaries may choose to attack vital technology infrastructure in an effort to obtain an advantage or cause harm. Numerous fields, such as critical infrastructure, communication networks, cybersecurity, weapon systems, and information systems, are susceptible to these vulnerabilities.

Second requirement: Serious Repercussions Technological Vulnerabilities

Exploiting technology flaws in armed situations can have serious repercussions, including:

First section: Disruption of Communication Networks: Adversaries may attempt to interfere with command and control systems by targeting communication networks, which will impede armed forces' ability to coordinate and respond.

Second section: Cyberattacks: Cyberattacks on civilian and military infrastructure can result in sabotage, data breaches, or the interruption of vital services, which can have an effect on both civilian and military activities.

Third section: Compromise of Weapon Systems: Weapon systems' vulnerabilities can be used to make them inoperable or even turn against their operators, putting personnel in peril and causing a loss of firepower.

Fourth section: Manipulation of Information: Propaganda or false information spread via technology can fool civilian or military populations, influencing public opinion of the conflict and decision-making processes.

Fifth section: Sabotage of Critical Infrastructure: Attacks against vital utilities like water supplies, transportation networks, or power grids can cause disruptions and pose logistical difficulties for military operations. ⁽⁸⁾

Second requirement: Security and Ethical issues of Technological Vulnerabilities

With the growing dependence of armed forces on developing technology and interconnected networks, these forces are vulnerable to manipulation and exploitation by adversaries. For example, new avenues for cyberattacks are opened up by the spread of Internet of Things (IoT) devices in military infrastructure. The potential threats posed by unsecured IoT ecosystems were highlighted in 2018 when the U.S. Navy's Naval Undersea Warfare Center was the victim of a cyber intrusion made possible by vulnerabilities in connected devices. ⁽⁹⁾

First section .Internet of Things (IoT)

The network of things appliances, cars, and other items that are implanted with sensors, software, and connection capabilities that allow them to gather and share data over the internet is known as the Internet of Things, or IoT. These gadgets might be anything from basic lightbulbs and thermostats for the home to intricate industrial gear and smart city infrastructure.

The goal behind the Internet of Things (IoT) is to build a network where common things can interact and communicate with humans and each other to perform tasks including automation, monitoring, and control. The development of intelligent systems that may boost productivity, facilitate new services, and improve efficiency in a number of industries, including manufacturing, transportation, healthcare, and agriculture, is made possible by this connectivity (10).

Furthermore, the development of autonomous weaponry. Although these technologies promise improved accuracy and fewer human casualties, they also give bad actors the chance to take advantage of weaknesses and control behavior. Autonomous weapons have sparked worries about the possibility of hacking or hijacking, which might have unexpected repercussions and escalate hostilities (11).

Second section:Risks of autonomous weaponry

In armed engagements, autonomous weapons raise a number of ethical, legal, and practical issues. The following major risks are backed up by scholarly citations and empirical references:

-Absence of Human Oversight: Since autonomous weapons function without direct human supervision, all decision-making is done by algorithms or artificial intelligence systems. The lack of human supervision may lead to erratic conduct and possible transgressions of human rights and international humanitarian law. (12).

- Risk of Targeting Non-Combatants and Civilians: Autonomous weapons may find it difficult to discriminate between combatants and civilians due to their lack of human-like judgment, which could result in indiscriminate attacks and civilian casualties . (13).

- Escalation of disputes: There is a chance that disputes will go out of control due to the speed and scope of autonomous weapons, which could have unforeseen repercussions and escalate bloodshed . ⁽¹⁴⁾.

-Incapacity to Ensure Compliance with International Law: Autonomous weapons could not be able to understand and abide by the intricate legal frameworks that regulate armed conflict, which could lead to possible transgressions of international law. ⁽¹⁵⁾.

- Accountability and Ethical Concerns: The use of autonomous weapons presents ethical issues regarding accountability and duty for their deeds, especially in the event of malfunction or unintentional injury. ⁽¹⁶⁾.

-Proliferation and Arms Races: The creation and application of autonomous weaponry may incite arms races among states vying for military supremacy, resulting in a rise in international unrest.

These concerns highlight the urgent need for strong international legislation and ethical frameworks to control the development and use of autonomous weapons in armed situations.

Conclusion

The emergence of digital threats in armed conflicts is a complex challenge that calls for an all-encompassing and flexible response. Prioritizing cybersecurity measures is crucial for governments and armies to protect vital infrastructure and reduce the likelihood of cyberattacks. Furthermore, there is a need to step up the fight against misinformation and propaganda, with a particular emphasis on media literacy and the protection of democratic ideals online.

Navigating the intricacies of modern warfare will also need addressing technological weaknesses and ethical issues with developing technologies. Through comprehension of the dynamic terrain of cyber threats and implementation of preemptive defensive tactics, countries can enhance their resilience against the hazards of the virtual front.

And we saw that Cyberattacks are intentional acts that target computer systems, networks, or data, causing damage, interrupting operations, or obtaining unauthorized access to private data. They are a powerful and pervasive form of aggression that can harm civilian populations, military installations, and vital services. The 2010 discovery of the infamous Stuxnet malware highlights the vulnerability of vital infrastructure to cyberattacks, with potentially disastrous results affecting military operations and large-scale power outages. State-

sponsored hacking groups, such as Fancy Bear from Russia and APT10 from China, have targeted government institutions and defense contractors, demonstrating the hazy distinction between cyberwarfare and conventional warfare.

Information warfare involves the deliberate use of information and communication technologies to alter behavior, shape perceptions, and further ideological, military, or political goals. It is a powerful instrument for rewriting history, swaying public opinion, and causing strife between enemies. Technological vulnerabilities are flaws or vulnerabilities in technological infrastructures or systems that can be used to alter, interfere with, or compromise their operation. These weaknesses can provide serious dangers in armed conflicts, as adversaries may choose to attack vital technology infrastructure to obtain an advantage or cause harm.

Technological vulnerabilities in armed situations can have serious consequences, including disruption of communication networks, cyberattacks, compromise of weapon systems, manipulation of information, and sabotage of critical infrastructure. The growing dependence of armed forces on technology and interconnected networks makes them vulnerable to manipulation and exploitation by adversaries. The Internet of Things (IoT) is a network of devices implanted with sensors, software, and connection capabilities that allow them to gather and share data over the internet. The development of autonomous weaponry in armed engagements raises ethical, legal, and practical issues.

The absence of human oversight in autonomous weapons can lead to erratic conduct and potential transgressions of human rights and international humanitarian law. It may also make it difficult to discriminate between combatants and civilians, leading to indiscriminate attacks and civilian casualties. Additionally, disputes may escalate due to the speed and scope of autonomous weapons.

In conclusion, technological vulnerabilities in armed situations pose significant security and ethical concerns for both military and civilian population

Citations:

1-Lindsay, J. R. (2013). "Stuxnet and the Limits of Cyber Warfare." *Security Studies*, 22(3), 365-404.

- 2-.Symantec. (2011). W32.Stuxnet Dossier. Retrieved from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
- 3-Langner, Ralph. "Stuxnet: Dissecting a Cyberwarfare Weapon." IEEE Security & Privacy, vol. 9, no. 3, May/June 2011, pp. 49-51
- 4- CrowdStrike. (2016 Intelligence Report: Putter Panda. Retrieved from https://www.crowdstrike.com/wp-content/brochures/Intel_Report_Putter_Panda.pdf
- 5- Rid, T. (2011). "Cyber War Will Not Take Place." Journal of Strategic Studies, 35(1), 5-32.
- 6- Mueller, R. S. (2019). Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Retrieved from <https://www.justice.gov/storage/report.pdf>
- 7- Rid, T. (2015). Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), 5-32.
- 8- Michael N. Schmitt and Liis Vihul: "Technological Vulnerabilities and Risks in Armed Conflicts" Source: "International Law Studies," Volume 93 (2017)
- 9- . ZDNet. (2018). Hackers breach US Navy, exposing sailors' personal data. Retrieved from <https://www.zdnet.com/article/hackers-breach-us-navy-exposing-sailors-personal-data/>
- 10- Atzori, Luigi, et al. "The Internet of Things: A survey." Computer Networks, vol. 54, no. 15, 2010, pp. 2787-2805.
- 11- Arkin, R. C. (2010). Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture. Technical Report No. 16-1. Retrieved from <https://apps.dtic.mil/sti/pdfs/ADA566467.pdf>
- 12- Arkin, R. C. (2009). Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture. In Robot Ethics (pp. 52-65). MIT Press.
- 13-Heyns, C. (2013). "Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions" United Nations General Assembly, Human Rights Council, Twenty-third session, Agenda item 3, UN Doc. A/HRC/23/47.

14- Horowitz, M. C., & Sagan, S. D. (2019). "The Causes and Consequences of Nuclear Weapons Proliferation" Annual Review of Political Science, 22, 67-86.

15 - Human Rights Watch. (2012). Losing Humanity:" The Case Against Killer Robots". Human Rights Watch.

16 - Sharkey, N. (2017). "The evitability of autonomous robot warfare" International Review of the Red Cross, 99(913), 699-717.

17- Scharre, P. (2018). "Army of None: Autonomous Weapons and the Future of War". W. W. Norton & Company.

Bibliography List:

1.Journal Articles:

1- Arkin, R. C. (2009). Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture. In Robot Ethics. MIT Press. (pp. 52-65)

2- Atzori, Luigi, et al. "The Internet of Things: A survey." Computer Networks, vol. 54, no. 15, 2010, pp. 2787-2805

3- Horowitz, M. C., & Sagan, S. D. (2019). "The Causes and Consequences of Nuclear Weapons Proliferation" Annual Review of Political Science, 22, 67-86.

4-Lindsay, J. R. (2013). "Stuxnet and the Limits of Cyber Warfare." Security Studies, 22(3), 365-404.

5-Langner, Ralph. "Stuxnet: Dissecting a Cyberwarfare Weapon." IEEE Security & Privacy, vol. 9, no. 3, May/June 2011, pp. 49-51

6- Michael N. Schmitt and Liis Vihul: "Technological Vulnerabilities and Risks in Armed Conflicts" Source: "International Law Studies," Volume 93 (2017)

7- Rid, T. (2011). "Cyber War Will Not Take Place." Journal of Strategic Studies, 35(1), 5-32.

8 - Sharkey, N. (2017). "The evitability of autonomous robot warfare" International Review of the Red Cross, 99(913), 699-717.

2.Reports:

1- Arkin, R. C. (2010). Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture. Technical Report No. 16-1. Retrieved from <https://apps.dtic.mil/sti/pdfs/ADA566467.pdf>

2- CrowdStrike. (2016) Intelligence Report: Putter Panda. Retrieved from https://www.crowdstrike.com/wp-content/brochures/Intel_Report_Putter_Panda.pdf

3-Heyns, C. (2013). "Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions" United Nations General Assembly, Human Rights Council, Twenty-third session, Agenda item 3, UN Doc. A/HRC/23/47.

4 - Human Rights Watch. (2012). Losing Humanity:" The Case Against Killer Robots". Human Rights Watch.

5- Mueller, R. S. (2019). Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Retrieved from <https://www.justice.gov/storage/report.pdf>

3. Internet websites:

1-.Symantec. (2011). W32.Stuxnet Dossier. Retrieved from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

2- . ZDNet. (2018). Hackers breach US Navy, exposing sailors' personal data. Retrieved from <https://www.zdnet.com/article/hackers-breach-us-navy-exposing-sailors-personal-data/>