

Achieving Cybersecurity in Light of Select Arab and Western Strategies

تحقيق الأمن السيبراني على ضوء بعض الاستراتيجيات العربية والغربية

Abbes Sadeki¹,

¹ University Center of Illizi,(Algeria), sadeki.abbes@cuillizi.dz

Received: 23/06/2022026

Accepted: 29/06/2026

Published 30./06/2026

Abstract:

This paper examines Arab and Western cybersecurity strategies, focusing on Egypt, Jordan, Saudi Arabia, the UK, Canada, and Germany, alongside international legal frameworks. It addresses whether international criminal law and universal jurisdiction can effectively counter cyber threats. The study finds broad consensus on five legislative solutions: prevention, international cooperation, urgency, integration with defense policies, and specialized training. It argues that large-scale cyberattacks challenge traditional legal categories, necessitating reconsideration of the laws of war and international justice. The *Tallinn Manual 2.0* emerges as the most authoritative reference for applying international law to cyber operations, though it remains non-binding on states.

Keywords: Cybersecurity; National Strategies; Cybercrimes, International Cooperation, International Criminal Law, Universal Jurisdiction, Cyber Warfare, Tallinn Manual 2.0.

JELClassificationCodes: k4; O2.

ملخص:

يهدف هذا المقال إلى تحليل استراتيجيات تحقيق الأمن السيبراني في بعض الدول العربية والغربية، واستكشاف آفاق التعاون الدولي في مكافحة الجرائم والتهديدات الإلكترونية. ويعالج إشكالية رئيسية مفادها: ما أهم محاور الاستراتيجيات العربية والغربية لتحقيق الأمن السيبراني، وما مدى إمكانية تطبيق قواعد القانون الجنائي الدولي والاختصاص القضائي العالمي لمكافحة التهديدات الإلكترونية؟

وتوصل المقال إلى أن هناك إجماعاً على خمسة حلول تشريعية كبرى، وأن الهجمات الإلكترونية الواسعة تطرح إمكانية إعادة النظر في تطبيق قواعد الحرب والعدالة الدولية عليها، مع الإشارة إلى " دليل تالين 2.0" كأهم مرجع قانوني في هذا المجال.

الكلمات المفتاحية العربية: الأمن السيبراني؛ الاستراتيجيات الوطنية؛ الجرائم الإلكترونية؛ التعاون الدولي؛ القانون الجنائي الدولي؛ الاختصاص القضائي العالمي؛ الحرب السيبرانية؛ دليل تالين.

تصنيفات JEL : O2 ; k4.

Corresponding author: Abbas Sadeki: sadeki.abbes@cuillizi.dz

1. INTRODUCTION

Cyberspace has emerged as a new arena of conflict and competition, no less dangerous than traditional battlefields—and perhaps even surpassing them in complexity and reach. Threats in this domain transcend geographic and international borders in record time, placing the national security of states, including Algeria, before unprecedented challenges. Hence the critical importance of this topic: the absence of a clear national cybersecurity strategy, or failure to keep pace with evolving international cooperation mechanisms, may render a state vulnerable to cyber extortion, interference in its internal affairs, or even the paralysis of its vital infrastructure.

Given the imperative need to develop cyber defense mechanisms, the core research problem of this paper crystallizes in the following main question: What are the most prominent axes of national strategies (Arab and Western) for achieving cybersecurity, and to what extent can international criminal law and the rules of universal jurisdiction frame the prospects for international cooperation in combating cybercrimes and electronic threats?

To address this research problem, this paper adopts the descriptive-analytical approach to monitor and analyze the components of various strategies, in addition to the comparative approach to identify points of convergence and divergence among them, supplemented by the legal approach to examine legislative frameworks and relevant rules of international law.

Section One: This section analyzes strategies for achieving cybersecurity by examining the key axes of Arab strategies (Egypt, Jordan, Saudi Arabia) and Western strategies (the United Kingdom, Canada, Germany), then distills the major consensual legislative proposals and solutions.

Section Two: This section reviews the prospects for international cooperation in combating cybercrimes and electronic threats by discussing the extent to which these crimes can be subjected to the rules of international criminal law and the principle of universal jurisdiction, with a focus on developments in the concept of "cyber warfare" and its potential impact as a legal reference.

II. Section One: Strategies for Achieving Cybersecurity

According to the NATO Cooperative Cyber Defence Centre of Excellence¹, countries worldwide have adopted dedicated cybersecurity strategies, including six Arab states: Jordan, Qatar, the Kingdom of Saudi Arabia, the United Arab Emirates, Egypt, and Morocco. What, then, are the main axes of these strategies, and what are the key legislative proposals and solutions they have collectively agreed upon to confront cybercrimes and electronic threats?

First: Key Axes Adopted by Select Arab Strategies for Achieving Cybersecurity

1. The Arab Republic of Egypt:

The Arab Republic of Egypt formulated its "Egyptian Strategy for Communications and Information Technology 2012–2017,"² which included among its components the integration of three fundamental axes into legislation: protecting cyberspace from threats, mandating public and private entities to secure their electronic communications, and activating oversight of cyberspace. These axes were introduced following the initial strategy (2007–2010). It is worth noting that the long-term strategy (2030)³, currently being implemented by the Ministry of Communications and Information Technology, is fundamentally oriented toward ensuring

¹ NATO Cooperative Cyber Defence Centre of Excellence. (Date of view 14-6-2026 Time 6:40) Available on the website: <https://ccdcoc.org/index.html>

² Arab Republic of Egypt, Ministry of Communications and Information Technology, "Egyptian Strategy for Communications and Information Technology 2007–2010" (Cairo: MCIT, 2007), available at: <http://www.mcit.gov.eg/Upcont/Documents/Egypt-ICT-Strategy.pdf> (accessed: 8 August 2017, 1:00).

³ Arab Republic of Egypt, Ministry of Communications and Information Technology, "Egypt Strategy for Communications and Information Technology 2030" (Cairo: MCIT, 2016), available at: http://www.mcit.gov.eg/Ar/ICT_Strategy (accessed: 8 August 2017, 1:00).

cyberspace security and maximizing the benefits of electronic communications in both the economic and social spheres.

2. *The Hashemite Kingdom of Jordan:*

The Hashemite Kingdom of Jordan issued its National Strategy for Information Security and Cybersecurity, which recommended "the establishment of a joint committee composed of representatives from the Ministry of Media and Communications Technology and experts from the Ministry of Justice to study and scrutinize legislation related to information network security." It further recommended that private sector institutions "establish internal systems and arrangements consistent with state legislation to enhance information security and prevent electronic threats".⁴

3. *The Kingdom of Saudi Arabia:*

In 2011, the Kingdom of Saudi Arabia developed a strategy for information technology development and cybersecurity, placing among its core axes an emphasis on security and judicial cooperation with various other states, and working to overcome procedural obstacles in combating all forms of cybercrime. The strategy also relied on information-sharing cooperation, particularly during crises, and proposed the establishment of a dedicated department tasked with formulating specific procedural rules to guide security and judicial bodies in achieving cooperation between national and foreign authorities regarding mutual legal assistance and exchange.⁵

Second: Key Axes Adopted by Select Western Strategies for Achieving Cybersecurity

1. *The United Kingdom:*

The United Kingdom Government issued its National Cyber Security Strategy 2016–2021⁶. As stated therein: "Even when key individuals responsible for the most harmful cyber criminal activity against the UK are identified, it is often difficult for the UK and relevant international law

⁴ Hashemite Kingdom of Jordan, "National Information Assurance and Cyber Security Strategy (NIACSS)" (Amman: Ministry of Information and Communications Technology, 2012), available at:

http://www.trc.gov.jo/EchoBusV3.0/SystemAssets/PDF/AR/StrategiesandPolic/Strategies/NIACS_S.pdf (accessed: 14 August 2017, 8:00).

⁵ Kingdom of Saudi Arabia, "Developing National Information Security Strategy for the Kingdom of Saudi Arabia" (Riyadh: Ministry of Communications and Information Technology, 2011).

⁶ United Kingdom Government, "National Cyber Security Strategy 2016–2021" (London: Cabinet Office, 2016), p. 45, available at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (accessed: 10 August 2024, 9:40).

enforcement agencies to prosecute them, particularly when they are located in a non-cooperative jurisdiction". Consequently, "the focus should be on countering electronic threats, whereby intelligence agencies, the Ministry of Defence, the police, and the National Crime Agency, in coordination with international partner agencies, will expand their efforts to identify, anticipate, and disrupt hostile cyber activity conducted by foreign state actors, cybercriminals, and terrorists. This will enhance intelligence gathering and exploitation with the aim of obtaining proactive intelligence and identifying adversary capabilities and intentions".

2. Canada:

Canada's cybersecurity strategy states: "The third pillar of Canada's Cyber Security Strategy focuses on providing Canadians with information to protect themselves and their families online, and on strengthening the ability of law enforcement agencies to combat cybercrime"⁷. To realize this objective, the Canadian government is working to "improve the legislative tools to better protect Canadians in cyberspace," having already begun, since early 2010, to enact legislation concerning user data protection and the prevention of malicious messages and spam.

3. Germany:

Germany has issued its White Paper on Security Policy and the Future of the Bundeswehr, within which it has formulated a comprehensive plan to address cyber challenges and threats. It has established "a common understanding of the application of international law" and resilience in response to these threats, in partnership with the European Union and NATO, as the cornerstone of achieving cybersecurity⁸. The German strategy also places significant emphasis on protection as a vital and essential factor in achieving security and confronting various manifestations of crime.⁹

Third: Consensual Legislative Proposals and Solutions in Cybersecurity Strategies

Examining the aforementioned strategies, it can be asserted that the legislative proposals and solutions upon which they have converged are as follows:

1. Emphasis on the Importance of Prevention:

⁷ Government of Canada, "Action Plan 2010–2015 for Canada's Cyber Security Strategy" (Ottawa: Public Safety Canada, 2010), available at: <https://www.securitepublique.gc.ca/cnt/rsracs/pblctns/ctn-pln-cbr-scrct/ctn-pln-cbr-scrct-eng.pdf> (accessed: 16 August 2024, 9:30).

⁸ Federal Ministry of Defence of Germany, "The White Paper on Security Policy and the Future of the Bundeswehr" (Berlin: BMVg, 2016), p. 78.

⁹ *Ibid.*, p. 82.

This is achieved by advocating for the adoption of legislative and procedural rules that expand crime prevention measures, making them a fundamental element of cybersecurity; by mandating both the public and private sectors to implement electronic protection systems against malware and viruses; by allocating specialized intelligence and investigative units within security and defense bodies; and by activating early warning systems for threats¹⁰. This should be accompanied by empowering these bodies with oversight and data access authorities under judicial supervision, in addition to implementing public awareness programs that equip citizens to protect themselves from electronic threats.

2. Emphasis on the Importance of Cooperation Between Security and Judicial Bodies at the National and International Levels:

This is realized by activating and energizing bilateral and multilateral cooperation instruments, responding swiftly to information-exchange requests between states, and enacting appropriate legislation to ensure the pursuit and prosecution of criminals.

3. Emphasis on the Urgent Nature of Combating Cybercrimes:

This involves amending criminal procedure codes, granting security and judicial authorities broader powers to pursue and counter cybercrimes and threats, and simplifying the procedures for obtaining authorization for searches, inspections, and the tracing of electronic information, while establishing clear safeguards that ensure respect for personal rights and freedoms.

4. Emphasis on Linking Policies for Combating Cybercrimes and Threats with Defense Policies and Strategies:

This entails involving military and defense institutions and their affiliated bodies in the development of legal frameworks that define the limits of their powers and contributions to protecting the cybersecurity of civilians and public and private sector institutions. This is particularly pertinent given the difficulty, in many cases, of distinguishing between a cybercrime targeting an individual or a group of individuals, and attacks or threats that result in the disruption of state security and the stability of its institutions.

5. Emphasis on the Training and Capacity-Building of Personnel Tasked with Combating Cybercrimes:

¹⁰ Prof. Dr. Abdelmadjid Zaâlani, "The Recognized Status of the Idea of Crime Prevention in Contemporary Penal Legislation in Algeria," *Algerian Journal of Law and Justice*, Ministry of Justice, Pilot Issue (2015), p. 9 (translated from Arabic).

This underscores the necessity of combining technical expertise with appropriate legal training, and ensuring their commitment to the boundaries of crime-fighting without transgressing legal safeguards that guarantee freedom of access to electronic services and the inviolability of private life, while also preserving the secrets and data of public and private institutions.

III. Section Two: Prospects for International Cooperation in Combating Cybercrimes and Electronic Threats between the Rules of International Criminal Law and the Rules of Universal Criminal Jurisdiction

International criminal law is defined as "a body of international rules designed to prohibit war crimes, crimes against humanity, genocide, aggression, torture, and international terrorism, to attribute responsibility to individuals who engage in such crimes, and to regulate the procedures before international criminal tribunals".¹¹ It is an existing body of law specifically concerned with establishing rules for combating international crimes and protecting the international public order. As for the rules of universal criminal jurisdiction, they are rules that have emerged from certain international practices, whereby states, through their national judicial bodies, may prosecute perpetrators of universal crimes—which are essentially domestic crimes that affect fundamental human and humanitarian values, such as war crimes and crimes classified as crimes against humanity [13]. The question has been raised as to whether it is possible to address cybercrimes and electronic threats from the perspective of international criminal law—that is, can states prosecute and try individuals accused of committing cybercrimes on the basis of the "crimes against humanity" or "war" character of such crimes, given that they affect the humanitarian values that the international community seeks to enshrine?

First: The Origins of the Principle of Universal Jurisdiction over Criminals

It is worth noting, at the outset, that one of the applications of the idea of "universal" prosecution of criminals for crimes against humanity is the Pinochet case, in which the Spanish judiciary exercised its authority to order the arrest of Pinochet for crimes most of which were committed in Chile, and most of whose victims were Chilean nationals. This authority is based on the rule of "universal jurisdiction"—the principle which holds that it is in the interest of every state to bring to justice the perpetrators of certain crimes that concern the international community as a whole,

¹¹ Antonio Cassese, *International Criminal Law*, 3rd ed. (Oxford: Oxford University Press, 2013), translated into Arabic by Sader Publishers (Beirut: Sader, 2015), p. 43.

regardless of where the crime was committed, and regardless of the nationality of the perpetrators or the victims. Jurisdiction over a crime is ordinarily based on the link between the prosecuting state and the crime itself, which is typically a territorial link; "however, in the case of crimes against humanity," as one senior lawyer has explained, "it is sufficient that this link is that we are all members of the human family".¹² The primary substantive reason for international law to stipulate universal jurisdiction is to ensure that no "safe haven" is available to those responsible for the most serious crimes.

Historically, piracy was the archetypal "universal" crime, to which the slave trade was later added. However, both of these crimes were committed across state borders or on the high seas. The number of crimes requiring universal jurisdiction has increased since the end of the Second World War, and the list has expanded to include many atrocities committed within national borders, such as genocide, torture, apartheid, and other "crimes against humanity". A landmark case heard by a United States court—the *Filártiga* case—stands as a milestone in judicial history. In that case, the family of a Paraguayan national who had been a victim of torture and subsequently moved to the United States brought a civil action against his torturer, who had also moved to the United States. The court ruled: "The torturer has become, like the pirate and the slave trader before him, an enemy of all humankind".¹³

Second: Are Cybercrimes and Cyberattacks Subject to the Rules of War and Universal Jurisdiction?

Many cybercrimes transcend the category of crimes affecting a small number of people or a specific group, evolving into cyber wars or attacks, exemplified by the large-scale attack that affected over 100 countries worldwide in May 2017.

Serious attempts have been made to link such attacks to crimes against humanity¹⁴, in an effort to determine the boundaries of applicability of the

¹² Counsellor Ashraf Mohamed Lashin, *The Supremacy of International Criminal Law* (Manama: Security Media Center, Kingdom of Bahrain), p. 7, available at: <https://www.policemc.gov.bh/mcms-store/pdf/18> (accessed: 22 August 2024, 8:00).

¹³ Jorge Arrate, "Pinochet's Trial, Chile's Dignity," *Project Syndicate*, 5 January 2005, available at: <https://www.project-syndicate.org/commentary/pinochet-s-trial--chile-s> (accessed: 19 August 2024, 9:30).

¹⁴ Oona A. Hathaway & Rebecca Crootof, "The Law of Cyber-Attack," *California Law Review*, Vol. 100, 2012, pp. 839–840, available at: http://digitalcommons.law.yale.edu/fss_papers (accessed: 25 August 2022, 11:30).

provisions of the law of war to this new category of crimes, and to fill the legal vacuum at the international level [19]. These attempts have involved measuring the damage resulting from war crimes and crimes against humanity in their traditional forms against that which could result from cyber wars and attacks, and examining the legitimacy of the hypothesis of responding to them with a counter-cyberattack "within the framework of just war theory"—a theory that justifies the use of force and recourse to war on the basis of certain ethical grounds and justifications, although it should be noted that the latter theory does not provide a comprehensive theoretical framework for cyberattack.¹⁵

These efforts have not been limited to theoretical and academic endeavors. In November 2011, the U.S. Department of Defense issued a report declaring its intention to use all necessary means to protect U.S. national security by securing cyberspace, including the use of military means allocated for electronic defense. The report stated:

"We will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we reserve the right to use all necessary means—diplomatic, informational, military, and economic—to defend our Nation, our Allies, our partners, and our interests. In doing so, we will exhaust all options prior to using force whenever we can; we will carefully weigh the costs and risks of action against the costs of inaction; and we will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support wherever possible. For its part, DoD will ensure that the U.S. military continues to have all necessary capabilities in cyberspace to defend the United States and its interests, as it does across all domains".¹⁶

From the foregoing, it appears that the expanding scope of electronic threats facing states will compel them to explore legal mechanisms capable of ensuring their security and safety, whether through the connection of such threats to the interests of a specific state, or their relation to international or regional public order—even if this necessitates deriving

¹⁵ Hamdi El-Sharif, *Just War Theory Between Utopia and Ideology* (Rabat: Mominoun Without Borders for Research and Studies, 18 April 2016), p. 3, available at: <http://www.mominoun.com/pdf1/2016-02/youtoubia.pdf> (accessed: 20 August 2024, 12:00).

¹⁶ United States Department of Defense, "Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934" (Washington, D.C.: DoD, November 2011), p. 3, available at: <http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf> (accessed: 19 August 2024, 12:30).

frameworks from the rules of international criminal law and establishing the legitimacy of countering global-scale electronic threats and attacks. This would give rise to a new form of defense, namely electronic or cyber defense, based on securing cyberspace and protecting it from potential threats that affect the interests of peoples and states in a manner comparable to war crimes and crimes against humanity. This approach is reinforced by the fact that cyberattacks target the electronic and computer systems of hospitals, transportation networks, and educational institutions. The International Committee of the Red Cross (ICRC) has affirmed that "the term 'cyber warfare' is used here to refer to means and methods of combat consisting of operations in cyberspace that amount to, or are conducted in the context of, armed conflict within the meaning of international humanitarian law. The ICRC is concerned about cyber warfare because of the vulnerability of electronic networks and the potential human cost of cyberattacks. When a state's computers or networks are attacked, hacked, or disrupted, this may expose civilians to the risk of being deprived of essential needs such as drinking water, medical care, and electricity. If GPS systems are disabled, civilian casualties may occur through, for example, the disruption of rescue helicopter operations. Dams, nuclear plants, and aircraft control systems may be vulnerable to cyberattacks due to their reliance on computers. Networks are so interconnected that it is difficult to limit the effects of a cyberattack against one part of the system without damaging other parts or disrupting the entire system. The welfare, health, and even lives of hundreds of thousands of people may be at risk. The ICRC reminds all parties to conflict to constantly take care to spare civilian lives—one of its most important roles—for war has rules and limits that apply to recourse to cyber warfare to the same extent as they apply to the use of rifles, artillery, and missiles".¹⁷

Finally, reference should be made to the efforts undertaken by a group of nineteen (19) international law experts and legal advisors specializing in cybercrime¹⁸, who provided a comprehensive and thorough analysis of how existing international law applies in cyberspace. This work was first

¹⁷ International Committee of the Red Cross (ICRC), "What are the Limits of the Law of War on Cyber Attacks?" 28 June 2013, available at: <https://www.icrc.org/ara/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm> (accessed: 30 August 2024, 12:00).

¹⁸ Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge: Cambridge University Press, 2017), available at: <https://ccdcoe.org/research.html> (accessed: 30 August 2017, 12:30).

published in 2013 by the University of Cambridge in cooperation with NATO, and was revised and updated in 2017 under the title *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. The purpose of this manual is to identify the rules governing cyber warfare. As stated in its introduction, "it is a manual compiling the views of experts and specialists and is not binding on states or on NATO". It addresses several key points, including sovereignty and jurisdiction, international criminal responsibility for cyber operations, provisions of international telecommunications law and state obligations, and cyberattack and its effects.¹⁹

IV. Conclusion:

Having examined select state strategies for achieving cybersecurity and the content of international law in the field of cybersecurity, a number of conclusions can be drawn, which are presented as follows:

First: Regarding Strategies for Achieving Cybersecurity

1. There is a clear convergence between Arab and Western strategies around five major axes: prevention, international cooperation, urgency, the integration of cyber policies with defense policies, and investment in training and capacity-building.
2. The substantive difference lies not in principles, but in implementation mechanisms and inter-institutional coordination. Western models (particularly the United Kingdom and Germany) excel in integrating the private sector and intelligence agencies into a unified national effort, whereas Arab strategies are still in the process of operationalizing these mechanisms.

Second: Regarding the Prospects for International Cooperation and International Criminal Law

1. The study has demonstrated that applying the principle of "universal jurisdiction" to cybercrimes faces significant procedural and legal difficulties. Cybercrimes—in their current characterization—do not automatically rise to the level of "crimes against humanity" unless they deliberately create catastrophic humanitarian conditions (such as attacks on nuclear facilities or hospitals), a criminal intent that is difficult to prove.

¹⁹ *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), pp. v–vi, available at: http://assets.cambridge.org/97811071/77222/excerpt/9781107177222_excerpt.pdf (accessed: 31 August 2024, 12:00).

2. Nevertheless, the *Tallinn Manual 2.0* stands as a monumental step toward establishing a unified legal framework, albeit non-binding, for cyber warfare. This paves the way for the international community to formulate a future international treaty on this type of conflict.
3. Recent orientations, coupled with the ICRC's concerns, confirm that the world has effectively entered the era of "armed cyber defense," where the right to military response to a large-scale cyberattack has become a viable option.

V . References

I. Books

1. Cassese, A. (2013), *International Criminal Law*, 3rd ed., Oxford: Oxford University Press. [Translated into Arabic by Sader Publishers (2015), Beirut: Sader, p. 43].
2. Lashin, A. M. (n.d.), *The Supremacy of International Criminal Law*, Manama: Security Media Center, Kingdom of Bahrain, p. 7. Available at: <https://www.policemc.gov.bh/mcms-store/pdf/18> (accessed: 22 August 2024, 8:00).
3. Schmitt, M. N. (Ed.) (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., Cambridge: Cambridge University Press.

II. Articles in Journals

4. Hathaway, O. A. & Crootoof, R. (2012), « The Law of Cyber-Attack », *California Law Review*, Vol. 100, pp. 817–885. Available at: http://digitalcommons.law.yale.edu/fss_papers (accessed: 25 August 2017, 11:30).
5. Zaâlani, A. (2015), « The Recognized Status of the Idea of Crime Prevention in Contemporary Penal Legislation in Algeria », *Algerian Journal of Law and Justice*, Ministry of Justice, Pilot Issue, p. 9. (No national legal texts were cited in this paper.)

III. Official Reports, Strategies, and Government Documents

6. Arab Republic of Egypt, Ministry of Communications and Information Technology (2007), *Egyptian Strategy for Communications and Information Technology 2007–2010*, Cairo: MCIT. Available at: <http://www.mcit.gov.eg/Upcont/Documents/Egypt-ICT-Strategy.pdf> (accessed: 8 August 2017, 1:00).

7. Arab Republic of Egypt, Ministry of Communications and Information Technology (2012), *Egyptian Strategy for Communications and Information Technology 2012–2017*, Cairo: MCIT. Available at: <http://mcit.gov.eg/Upcont/Documents/ICT%20Strategy%202012-2017.pdf> (accessed: 8 August 2024, 1:00).
8. Arab Republic of Egypt, Ministry of Communications and Information Technology (2016), *Egypt Strategy for Communications and Information Technology 2030*, Cairo: MCIT. Available at: http://www.mcit.gov.eg/Ar/ICT_Strategy (accessed: 8 August 2017, 2:00).
9. Federal Ministry of Defence of Germany (2016), *The White Paper on Security Policy and the Future of the Bundeswehr*, Berlin: BMVg.
10. Government of Canada, Public Safety Canada (2010), *Canada's Cyber Security Strategy*, Ottawa: Public Safety Canada.
11. Government of Canada, Public Safety Canada (2010), *Action Plan 2010–2015 for Canada's Cyber Security Strategy*, Ottawa: Public Safety Canada. Available at: <https://www.securitepublique.gc.ca/cnt/rsrscs/pblctns/ctn-pln-cbr-scrct/ctn-pln-cbr-scrct-eng.pdf> (accessed: 16 August 2024, 9:30).
12. Hashemite Kingdom of Jordan, Ministry of Information and Communications Technology (2012), *National Information Assurance and Cyber Security Strategy (NIACSS)*, Amman: MCIT. Available at: <http://www.trc.gov.jo/EchoBusV3.0/SystemAssets/PDF/AR/Strategi esandPolic/Strategies/NIACSS.pdf> (accessed: 14 August 2017, 8:00).
13. Kingdom of Saudi Arabia, Ministry of Communications and Information Technology (2011), *Developing National Information Security Strategy for the Kingdom of Saudi Arabia*, Riyadh: MCIT.
14. United Kingdom Government, Cabinet Office (2016), *National Cyber Security Strategy 2016–2021*, London: Cabinet Office. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (accessed: 10 August 2017, 9:40).
15. United States Department of Defense (November 2011), *Department of Defense Cyberspace Policy Report: A Report to Congress*

Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, Washington, D.C.: DoD, p. 3. Available at: <http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf> (accessed: 19 August 2017, 12:30).

IV. International Reports, Legal Sources, and Case Law

16. Arrate, J. (5 January 2005), « Pinochet's Trial, Chile's Dignity », *Project Syndicate*. Available at: <https://www.project-syndicate.org/commentary/pinochet-s-trial--chile-s-> (accessed: 19 August 2024, 9:30).
17. El-Sharif, H. (18 April 2016), *Just War Theory Between Utopia and Ideology*, Rabat: Mominoun Without Borders for Research and Studies, p. 3. Available at: <http://www.mominoun.com/pdf1/2016-02/youtoubia.pdf> (accessed: 20 August 2017, 12:00).
18. Filártiga v. Peña-Irala, 630 F.2d 876 (2d Cir. 1980). Available at: <http://thewonder.my-goo.net/t10953-> (accessed: 22 August 2024, 1:20).
19. Garcés, J. (1998), Statement cited in *Re: Pinochet*, Spanish National Court, Criminal Chamber.
20. International Committee of the Red Cross (ICRC) (28 June 2013), « What are the Limits of the Law of War on Cyber Attacks? » Available at: <https://www.icrc.org/ara/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm> (accessed: 30 August 2022, 12:00).
21. International Law Commission (ILC) (1996), « Draft Code of Crimes against the Peace and Security of Mankind », *Yearbook of the International Law Commission*, Vol. II, p. 15.
22. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (n.d.), « Cybersecurity Strategy Documents ». Available at: <https://ccdcoe.org/cyber-security-strategy-documents.html> (accessed: 8 August 2024).
23. Perlroth, N. (14 May 2017), « What We Know About the Global Ransomware Attack », *The New York Times*.
24. Schmitt, M. N. (Ed.) (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press, pp. v–vi. Excerpt available at: http://assets.cambridge.org/97811071/77222/excerpt/9781107177222_2_excerpt.pdf (accessed: 31 August 2022, 12:00).

V. Online Resources and Websites

25. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (n.d.), « Cybersecurity Strategy Documents ». Available at: <https://ccdcoe.org/cyber-security-strategy-documents.html> (accessed: 8 August 2024).