CYBERWAR AND CYBERTERRORISM. FEATURES AND ANSWERS TO THESE THREATS

Colonel (r.) Romică CERNAT, PhD

In recent years, cyberspace has taken increased strategic importance as states have begun to think of it as a domain similar to land, sea, and air, that must be secured to protect their national interests. Cyberattacks are now a common element of international conflict, both on their own and in the broader context of military operations. Attacks in cyberspace have been amplified and diversified in terms of actors and methods. Because states have become more dependent on information technology and critical network infrastructure components, many questions arise about whether a state is organised properly to defend its digital strategic assets. Cyberspace integrates the operation of critical infrastructures, as well as governmental and national security institutions and commerce. Because cyberspace transcends geographic boundaries, much of it is outside of control and influence of a state.

Keywords: cyberwar, cyberterrorism, cybercrime, computer virus, computer network, information system.

PRELIMINARY CONSIDERATIONS

The concept of *"Cyber-attack"* is a relatively recent term and refers to a wide range of activities conducted through the use of information and communication technology (ICT). The use of Distributed Denial of Service (DDoS) attacks has become a widespread method of achieving political objectives through the disruption of online services. In this type of attacks, a server is overwhelmed with Internet traffic so that access to certain websites is degraded or denied. *Stuxnet* virus appearance, in June 2010, which some consider the first cyber-attack, revealed that cyber-attacks could have a destructive and lasting effect. Created to sabotage Iran's nuclear programme, Stuxnet, the destructive system of computer software, attacked the industrial computerised control systems on which nuclear centrifuges that produce enriched uranium operate, having as finality the physical self-destruction of the facilities. Recent international events have raised questions about the situation when a cyberattack could be considered an act of war and what kind of response options are available to the victim states.

Stuxnet virus appearance, in June 2010, which some consider the first cyber-attack, revealed that cyber-attacks could have a destructive and lasting effect. Created to sabotage Iran's nuclear programme, Stuxnet, the destructive system of computer software, attacked the industrial computerised control systems on which nuclear centrifuges that produce enriched uranium operate, having as finality the physical self-destruction of the facilities.

Given those presented above, it is necessary that each state should take the necessary measures and develop the mechanisms at the national level and participate, at the European and international level, in the field of networks and information security systems to ensure a common high level of security and boost cooperation in the domain[1].

The cyber-attacks on *Sony Entertainment* illustrate the difficulties in classifying attacks and formulating a policy response. On 24 November 2014, Sony Corporation has been the subject of a cyber-attack which disabled its ICT systems, destroyed data and workstations and accessed internal e-mails and other data. The Federal Bureau of Investigation (FBI) and the Director of National Intelligence (DNI) of the United States of America attributed the cyber-attacks to the North Korean government. North Korea denied involvement in the attack, but praised a hacktivist group called the *"Guardians of Peace"*

[1] *Law no. 362/2018 on ensuring a common level of security of networks and information systems*, in the *Official Gazette,* Part I no. 21 of 9 January 2019, p.1.

for having done a *"righteous deed"*. During a press conference on 19 December 2014, President Obama pledged to *"respond proportionally"* to North Korea's alleged cyber aggression *"in a place, time and manner of our choosing"*[2]. President Obama categorised the incident as an act of *"cyber-vandalism"*, while other analysts labelled it as an act of cyberwar.

This incident illustrates the difficulties in classifying cyber-attacks, with respect to the actors involved and their motivations, as well as issues of sovereignty regarding the site where the actors were physically located. With the globalised nature of the Internet, authors can launch cyber-attacks from anywhere in the world and direct the attacks through servers belonging to third-party countries. A deep analysis of major cyber-attacks on government agencies, companies in the defence sector and high-tech, or economic crime with losses of more than one million dollars highlights the extent of this phenomenon[3]. Was the cyber-attack on Sony, a private corporation with headquarters in Japan, an attack on the USA? Further, could it be considered an act of terrorism, use of force or a cybercrime? In categorising the attack on Sony as an act of *"cyber vandalism"*, which usually includes compromising websites and is generally the realm of politically motivated actors known as the *"hacktivists"*, President Obama had reservations about what kind of response could be considered *"proportional"* and against whom. Another potential question could be related to the circumstances under which the USA would commit troops to respond to a cyber-attack. In a logical relationship is also the question of whether the USA and other powerful states have an effective deterrent strategy in place. The US acting DNI, Clapper, said about cyberwar actors that *"if they get global recognition, at low cost and will no consequence, they will do it again and keep doing it again until we push back"*[4].

With the globalised nature of the Internet, authors can launch cyber-attacks from anywhere in the world and direct the attacks through servers belonging to third-party countries. A deep analysis of major cyber-attacks on government agencies, companies in the defence sector and high-tech, or economic crime with losses of more than one million dollars highlights the extent of this phenomenon.

[2] Barack Obama, *"Remarks by the President in Year-End Press Conference"*, 12 December 2014, in *The White House Office of the Press Secretary*, https://obamawhitehouse.archives.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference, retrieved on 20.12.2019.

[3] *"Significant Cyber Incidents Since 2006"*, in *Center for Strategic & International Studies*, https://csis-prod.s3.amazonaws.com/s3fs-public/200108_Significant_Cyber_Events_List.pdf?aj4_VlDq2hSan2U8O5mS29Iurq3 G1QKa, retrieved on 07.01.2020.

[4] Chris Strohm, *"FBI Provides More Proof of North Korea Link to Sony Hack"*, 7 January 2015, in *Bloomberg*, https://www.bloomberg.com/news/articles/2015-01-07/clapper-warns-of-more-potential-north-korean-hacks-after-sony, retrieved on 20.12.2019.

THE STATES AND INTERNATIONAL BODIES STANCE TO CYBERWARFARE

Critical infrastructure has long been subject to physical threats and is now increasingly exposed to the risk of attacks in cyberspace[5]. Cyberwar is typically conceptualised as state-on-state action equivalent to an armed attack or use of force in cyberspace that may trigger a military response with a proportional use of force. Criminals, terrorists and spies, in their work, rely heavily on cyber-based technologies to accomplish the organisational objectives. Cyber terrorists are individuals sponsored by state and non-state actors that engage in cyber-attacks to achieve their objectives. Transnational terrorist organisations, insurgents and jihadists have used the Internet as a tool for planning attacks, radicalisation and recruitment as a method of propaganda dissemination, and as a means of communication, as well as for disruptive purposes.

Cyber terrorists are individuals sponsored by state and non-state actors that engage in cyber-attacks to achieve their objectives. Transnational terrorist organisations, insurgents and jihadists have used the Internet as a tool for planning attacks, radicalisation and recruitment as a method of propaganda dissemination, and as a means of communication, as well as for disruptive purposes.

There are no clear criteria, yet, for determining whether a cyber-attack is a crime, an act of hacktivism, terrorism or the use of force by a state equivalent to an armed attack. Similarly, no international, legally binding instruments have been yet drafted, which explicitly regulate inter-state relations in cyberspace.

In September 2012, the US Department of State took a public stand on the fact that cyber-attacks could be interpreted as a use of force in accordance with Article 2, paragraph 4, of the UN Charter and customary International Law. According to the Legal Advisor of the Department of State at that time, Harold Koh, *"cyber activities that proximately result in death, injury or significant destruction would likely be viewed as a use of force"*[6]. The examples given in Koh's remarks included triggering the destruction of a nuclear power plant, opening a dam and causing flood damage or causing airplanes to crash by interfering with air traffic control. Focusing more on the effects produced rather than the means with which they are carried out, this definition of cyberwar integrates easily within the existing international legal framework. If an actor employs a cyber-mean to produce kinetic effects that could

[5] The White House, in *National Strategy for Counterterrorism of the United States of America*, October 2018, p. 19, https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf, retrieved on 20.12.2019.

[6] Harold Hongju Koh, *"International Law in Cyberspace"*, in *US Department of State*, *Archived content*, 18 September 2012, https://2009-2017.state.gov/s/l/releases/remarks/197924.htm, retrieved on 20.12.2019.

justify the use of military force in other circumstances, then the use of that weapon can be treated as use of force.

Koh explained that cyber-attacks on information networks during an ongoing armed conflict would be governed by the same principles of proportionality that apply to other actions under the law of armed conflict. These principles include retaliation in response to a cyber-attack with a proportional use of military force. In addition, *"computer network activities that amount to an armed attack or imminent threat"* may trigger a state's right to self-defence in accordance with Article 51 of the UN Charter provisions. Koh cites in his remarks the 2011 International Strategy for Cyberspace (ISC), which provides that *"when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country"*[7]. One of the defence objectives of ISC is to work internationally *"to encourage responsible behaviour and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend national assets"*[8]. A growing awareness of the environmental threats in cyberspace has led to two major international processes aimed at developing international expert consensus among international cyber authorities.

NATO regulations for cyberspace. A year after the 2007 DDoS attack on Estonia, NATO established the Cooperative Cyber Defence Centre of Excellence (CCDCE) in Tallinn, Estonia. CCDCE hosts workshops and courses of law and ethics in cyberspace, as well as cyber defence exercises. In 2009, the Centre convened an international group of independent experts to develop a manual to be approved by a law and regulate how to act in case of a cyber-war. The Tallinn Manual, as it is known, was published in 2013[9]. It sets out 95 *"written severe rules"* governing the consequences of cyber conflict in relation with the sovereignty and responsibility of the state, the law of armed conflict, humanitarian law and the law of neutrality. The Tallinn Manual is an academic text and although it offers reasonable justifications

The Tallinn Manual, as it is known, was published in 2013. It sets out 95 "written severe rules" governing the consequences of cyber conflict in relation with the sovereignty and responsibility of the state, the law of armed conflict, humanitarian law and the law of neutrality. The Tallinn Manual is an academic text and although it offers reasonable justifications for the implementation of international law, it is not binding, and the authors stress that they do not speak for NATO or the CCDCE.

[7] *"International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World"*, May 2011, in *US Department of State*, p. 14, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/ international_strategy_for_cyberspace.pdf, retrieved on 20.12.2019.

[8] *Ibidem*. p.12.

[9] *"Tallinn Manual on the International Law Applicable to Cyber Warfare"*, in *The NATO Cooperative Cyber Defence Centre of Excellence*, p. 5, http://csef.ru/media/articles/3990/3990.pdf, retrieved on 06.01.2020.

for the implementation of international law, it is not binding, and the authors stress that they do not speak for NATO or the CCDCE.

Arguably, NATO currently does not have a clear position on the application of Articles 4 and 5 of the NATO Treaty in cyberspace and presently does not define a cyber-attack as a clear military action. The Tallinn Manual equates a use of force to those cyber operations whose *"effects… are analogous to those that would result from an action otherwise qualifying as a kinetic armed attack"*[10]. If an attack is deemed to be orchestrated by a cyber-criminal organisation, whether politically or financially motivated, then it may be the attacked state responsibility to select an appropriate response within its jurisdiction. However, the transnational nature of most criminal organisations in cyberspace can complicate decisions on jurisdiction.

Law of armed conflict on cyberwar. Reprisals in response to armed attacks are permitted in international law, when a belligerent state violates international law during peacetime, or the law of armed conflict, during wartime. However, the term *"armed attack"* has no legal definition and is still open to interpretation, completion and change, with respect to cyber-attacks. The so-called *"Law of War"*, also known as the law of armed conflict, embodied in the Geneva and Hague Conventions and the UN Charter, may under certain circumstances apply to cyber-attacks, but no attempts recorded by the states to implement it, or the existence of specific agreements regarding the applicability, its relevance under these conditions remains unclear. The application becomes complicated, and also, because of the difficulties in attribution, the potential use of remote computers, as well as the possible harm to third parties resulting from cyber counterattacks, which could be difficult to be controlled or contain. In addition, territorial boundaries issues and what constitutes an armed attack in cyberspace remain. The law's enforcement would seem clearest in situations where a cyber-attack causes physical damage, such as disruption of electric grid. As mentioned above, the *Tallinn Manual* addresses many of these questions[11]. In the absence of a legal definition of what constitutes an *"armed attack"* in cyberspace,

In the absence of a legal definition of what constitutes an "armed attack" in cyberspace, Professor Michael Schmitt suggests the following criteria for analysis in accordance with international law: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy and responsibility.

[10] *Ibidem,* p.54.

[11] Oona A. Hathaway, *"The Law of Cyber-Attack",* in *California Law Review, Vol. 100, No. 4, 2012,* pp.6-23, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2134932, retrieved on 06.01.2020.

Professor Michael Schmitt suggests the following criteria for analysis in accordance with international law: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy and responsibility[12].

The basic principles contained in *The Hague Convention*, regarding the application of armed forces are those of military necessity, proportionality, humanity and chivalry. If a state's military is conducting cyber operations in accordance with these principles, it may be said to be engaging in a cyber-war.

Council of Europe's stance on cybercrime. In this context, *The Council of Europe Convention on Cybercrime* is the first international treaty that attempts to harmonise laws across countries as to what constitutes criminal activity in the cyber realm. This law enforcement treaty, also known as the *"Budapest Convention"*, requires signatories to adopt criminal laws against various types of activities in cyberspace, to empower law enforcement institutions to investigate such activities and to cooperate with similar agencies of other signatory states[13]. While it is widely recognised as the most substantial international agreement regarding cyber security, some observers consider it as unsuccessful[14]. Some critics warn that the Convention provisions are limited on the enforcement side and lacks corresponding legislation in all countries, so criminals can operate freely in this field. In addition, by September 2019, only 64 states have ratified it.

UN General Assembly resolutions relating to cyberspace. A series of UN General Assembly resolutions relating to cybersecurity have been adopted over the past 19 years. One resolution requested for the convening of a report from an international group of government experts from 15 states, including the USA. The stated goal of this process was to build a *"cooperation for a peaceful, secure, resilient and open ICT environment"* by reaching an agreement on the *"norms, rules and principles of responsible behaviour by States"* and identifying

A series of UN General Assembly resolutions relating to cybersecurity have been adopted over the past 19 years. One resolution requested for the convening of a report from an international group of government experts from 15 states, including the USA. The stated goal of this process was to build a "cooperation for a peaceful, secure, resilient and open ICT environment" by reaching an agreement on the "norms, rules and principles of responsible behaviour by States" and identifying capacity-building measures for confidence and capabilities, including for exchange of information.

[12] Katharina Ziolkowski, *"Ius ad bellum in Cyberspace – Some Thoughts on the <Schmitt-Criteria> for Use of Force"*, in *Legal & Policy Branch NATO CCD COE*, pp. 1-7, https://ccdcoe.org/uploads/2012/01/5_3_Ziolkowski_ IusAdBellumInCyberspace.pdf, retrieved on 06.01.2020.

[13] *"Convention on Cybercrime"*, Budapest, 23.XI.2001, in *Council of Europe, European Treaty Series-No. 185*, pp. 7-13, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId= 0900001680081561, retrieved on 06.01.2020.

[14] Jack Goldsmith, *"Cybersecurity Treaties: A Skeptical View"*, 2 June 2011, in *Future Challenges in National Security and Law,* edited by Peter Berkowitz, pp. 1-11, http://media.hoover.org/sites/default/files/documents/Future Challenges_Goldsmith.pdf., retrieved on 06.01.2020.

capacity-building measures for confidence and capabilities, including for exchange of information. Unlike the work done in Tallinn under the auspices of NATO, this US-led process included both China and Russia. The resulting 2010 report, sometimes referred to as the *Group of Governmental Experts Report* recommended a series of measures to *"reduce the risk of misperception resulting from ICT disruptions"*, but did not include any binding agreements[15].

Nevertheless, some analysts consider that the report represents progress in overcoming differences between the USA and Russia regarding various aspects of cybersecurity. In December 2001, the General Assembly approved Resolution 56/183, which endorsed the World Summit on the Information Society, to discuss information society opportunities and challenges. This Summit was convened for the first time in Geneva, in 2003, and then in Tunis, in 2005, and then, after 10 years, in Geneva, in May 2013. Delegates from 175 countries attended the first Summit, where they adopted a *Declaration of Principles* – a road map for achieving an open information society. The Geneva Summit has left other, more controversial problems unresolved, including the issue of Internet governance and funding. At both summits, proposals for the USA to give up control of the *Internet Corporation for Assigned Names and Numbers* were rejected. An international treaty banning cyberwar and the use of information as a weapon was proposed at the UN by the Russian and German delegations.

In December 2001, the General Assembly approved Resolution 56/183, which endorsed the World Summit on the Information Society, to discuss information society opportunities and challenges. This Summit was convened for the first time in Geneva, in 2003, and then in Tunis, in 2005, and then, after 10 years, in Geneva, in May 2013. Delegates from 175 countries attended the first Summit, where they adopted a Declaration of Principles – a road map for achieving an open information society.

Other international agreements regarding cyberwar. Some bodies of international law, especially those relating to aviation and the sea, may be applicable to cyber security, for example, by prohibiting the disruption of air traffic control or other conduct that might jeopardise aviation safety[16]. Bilateral plans, mutual legal assistance treaties between countries may be applicable for criminal investigations in cyber security and prosecution.

[15] United Nations Secretary-General, *"Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security"*, 30 July 2010, *United Nations General Assembly*, pp. 7-8, https://www.un.org/ga/search/view_doc.asp?symbol=A/65/201, retrieved on 06.01.2020.

[16] Oona A. Hathaway, *op. cit*. pp.11, 28, 31-32.

CYBERTERRORISM – CHARACTERISTIC FEATURES

As with cyberwarfare, in most national laws or in international law, there is no consensus definition of what constitutes cyberterrorism. Some definitions addressing terrorist acts that transcend borders refer to some activities and damage defined in the fraud and abuse in networks and information systems. An important aspect of these legal documents is the approach regarding *"punishment for an offense"*, which entails fines or imprisonment and suggests that the aggressor party has committed a criminal act rather than an act of terrorism, while others claim it is an act of war, whether committed by a state actor.

The USA considers it is illegal for an entity to "knowingly access a computer without authorisation or exceeding the level of authorised access, and by means of such conduct having obtained information, that has been determined by the Government, pursuant to a law, to require protection against unauthorised disclosure for reasons of national security or foreign relations or are restricted from other reasons, with reason to believe that such information so obtained could be used to injury the USA or can be used to the advantage of any foreign state".

For example, the USA considers it is illegal for an entity to *"knowingly access a computer without authorisation or exceeding the level of authorised access, and by means of such conduct having obtained information, that has been determined by the Government, pursuant to a law, to require protection against unauthorised disclosure for reasons of national security or foreign relations or are restricted from other reasons, with reason to believe that such information so obtained could be used to injury the USA or can be used to the advantage of any foreign state"*[17]. According to the FBI, the Internet and, in particular, the use of social media are among the key *"factors that have contributed to the evolution of the terrorism threat landscape"* since the terrorist attacks on 11 September 2001[18].

Some legal analyses define cyberterrorism as *"the premeditated use of disruptive activities or the threat thereof, against computers or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives"*[19]. However, these actions are also considered criminal and generally refer to individuals or organisations rather than to state actors. Some definitions of cyber terrorism focus on the distinction between the disruptive and destructive action, the terrorism generating fear comparable to that of physical attack

[17] H. Marshall Jarrett, *Prosecuting Computer Crimes*, in *Office of Legal Education Executive Office for United States Attorneys,* pp. 12-13, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ ccmanual.pdf, retrieved on 06.01.2020.

[18] FBI, *"Terrorism"* in *What We Investigate*, https://www.fbi.gov/investigate/terrorism, retrieved on 06.01.2020.

[19] Barry C. Collin, *"Cyberterrorism"*, in *Institute for Security and Intelligence*, *11th Annual International Symposium on Criminal Justice Issues*, p.1, https://www.nato.int/structur/library/bibref/cyberterrorism.pdf , retrieved on 06.01.2020.

and is not just a costly disaster. Although a DDoS attack itself does not produce this kind of fear or destruction, the problem is the potential for second or third order effects. For example, if the telecommunications and emergency services were completely inoperable in a time of crisis, the effects of that sort of infrastructure attack could be catastrophic. However, in this case, the emergency service system itself is most likely not a target, but rather the result of collateral damage to vulnerable telecommunications network. Since the 2007 attack on Estonia, NATO has established authorities relating to cyber defence, with the goals of advancing strategy and centralising defence capabilities across members. A policy on cyber defence and an associated action plan were adopted in 2011, and to facilitate the centralisation effort, the NATO Communications and Information Agency was established in 2012[20].

Characteristics of cyberterrorism. In specialised literature for analytical and statistical purposes, there are various definitions for the term *"cyber terrorism"*, just as various definitions exist for the term *"terrorism"*. Terrorism has been defined as premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence a certain community. Dorothy Denning, security expert, defines cyberterrorism as *"... politically motivated hacking operations into networks and intelligence data, intended to cause grave harm, such as loss of life or severe economic damages"*[21]. The US Federal Emergency Management Agency defines cyberterrorism as *"unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives"*[22].

In specialised literature for analytical and statistical purposes, there are various definitions for the term "cyber terrorism", just as various definitions exist for the term "terrorism". Terrorism has been defined as premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence a certain community.

Others analysts indicate that a physical attack that destroys computerised centres for critical infrastructure, such as the Internet, telecommunications, or electricity power grid, ever touching

[20] Olivier Kempf, *"NATO and Cyber Defense"*, in *NDC Research Paper*, article no. III.6, May 2013, p. 3, https://www.chaire-cyber.fr/IMG/pdf/nato_and_cyberdefense_olivier_kempf_05.2013.pdf , retrieved on 07.01.2020.

[21] Dorothy Denning, *"Activism, Hacktivism, and Cyberterrorism: The Internet As a Tool for Influencing Foreign Policy"* in *Nautilus Institute, Conference on "The Internet and International Systems"*, p. 3, https://www.rand.org/ content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf , retrieved on 06.01.2020.

[22] Sarah Gordon, *"Cyberterrorism?"*, in *Symantec White Paper*, July, 2002, p. 4, https://www.symantec. com/avcenter/reference/cyberterrorism.pdf , retrieved on 07.01.2020.

a keyboard, can also contribute to or be labelled as cyberterrorism[23]. The proportion of cybercrime that can be directly or indirectly attributed to terrorists is difficult to determine. However, there are links between terrorist groups and criminals, that allow terror networks to expand internationally through leveraging the information resources, money laundering activities, or transit routes operated by criminals[24]. Some experts estimate that advanced or structured cyber-attacks, against multiple systems and networks, including targets surveillance and testing of sophisticated new hacker tools, might require from two to four years of preparation, while a complex coordinated cyber-attack, causing mass disruption against integrated, heterogeneous systems, may require six to ten years of preparation[25].

Analysis circumstances on cyber terrorism. Distinctions between crime, terrorism and war tend to blur when attempting to describe a computer network attack (CNA) in ways comparative to other areas of social life. For example, if a state were to secretly sponsor nonstate actors that initiate a CNA to support terrorist activities or to create economic disruption, the distinction between cybercrime and cyberwar becomes less clear, because it is difficult to say from where a cyber-attack originates, taking into account that an attacker may direct suspicion toward an innocent third party. Likewise, the interactions between terrorists and criminals who use ICT may sometimes blur the distinction between cyber-crime and cyber terrorism.

There may also be the cases that individuals providing computers expertise to a criminal or terrorist may not be aware of the intentions of the individual that requested the support. In this context, it remains difficult to identify the sources responsible for most of the disturbing yet increasingly sophisticated attacks that compromise the Internet.

There may also be the cases that individuals providing computers expertise to a criminal or terrorist may not be aware of the intentions of the individual that requested the support. In this context, it remains difficult to identify the sources responsible for most of the disturbing yet increasingly sophisticated attacks that compromise the Internet.

[23] Edward V. Linden, *"Focus on Terrorism"*, in *Nova Science Publishers, Inc*, vol.9, p.6, https://books. google.ro/books?id=wl-Ds42YMDIC&pg=PA30&lpg=PA30&dq=Dan+Verton,+%E2%80%9CA+Definition+of+ Cyber-terrorism%E2%80%9D,+Computerworld,+August+11,+2003,+p.6&source=bl&ots= dRkvffLk4i&sig= ACfU3 U3wC6ltTKQ2aQM6vL-EkQ2bVKetYg&hl=ro&sa=X&ved=2ahUKEwjBoJaJsYbnAhVil4 sKHSzXB8wQ6AEw AH oECAoQAQ#v =onepage&q=Dan%20Verton%2C%20%E2%80%9CA%20Definition%20of%20Cyber-terrorism %E2 %80%9D%2C%20Computerworld%2C%20August%2011%2C%202003%2C%20p.6&f=false, retrieved on 07.01.2020.

[24] Rollie Lal, *"Terrorists and Organized Crime Join Forces"*, in *The New York Times*, May 24, 2005, p. 1, https://www.nytimes.com/2005/05/24/opinion/terrorists-and-organized-crime-join-forces.html, retrieved on 07.01.2020.

[25] Clay Wilson, *"Computer Attack and Cyberterrorism"*, in *Naval History and Heritage Command*, p. 17, https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/c/computer-attack-cyberterrorism-crs.html, retrieved on 07.01.2020.

Given the difficulty in determining the author of the intrusion or the cyber-attacks, some argue that, unlike responding to traditional criminal acts, the focus should be placed on the act rather than the perpetrator and the threshold for triggering defensive or offensive action should be lowered. The Internet was used as a prime recruiting tool for insurgents in Iraq[26]. Insurgents have created many Arabic language websites that had the responsibility to contain coded plans for new attacks. Some reportedly give advice on how to build and operate weapons, and how to cross border checkpoints[27]. Other news articles report that a younger generation of terrorists and extremists, such those behind the July 2005 bombings in London, are learning new technical skills to help them avoid detection by law enforcement ICT[28].

When is cyber-attack considered cyber terrorism? Some analysts believe that the term *"cyber terrorism"* is inappropriate because a widespread cyber-attack may simply produce disarray, suffering, not terror, as would produce a bomb or other chemical, biological, radiological or nuclear weapon. However, some analysts believe that the effects of a widespread computer networks attack would be unpredictable and might cause enough economic disruption, fear and civilian deaths, to qualify as an act of terrorism[29].

It may highlight at least two points of view to define the term cyber terrorism: effects based:, intent based.

So, it may highlight at least two points of view to define the term cyber terrorism:

1. *effects based*: cyberterrorism exists when information attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if committed by criminals;

2. *intent based*: cyberterrorism exists when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or certain personalities to promote a political agenda or to cause grave harm or severe economic damage.

Effectiveness of current legislation. Do the institutions in the field of security have the authority they need to effectively fight and win wars

[26] Jonathan Curial, *"Iraq's Tech-savvy Insurgents Are Finding Supporters and Luring Suicide-bomber Recruits over the Internet"*, in *San Francisco Chronicle*, 10 July 2005, pp. 1-3, https://www.sfgate.com/news/article/TERROR-COM-Iraq-s-tech-savvy-insurgents-are-2623261.php, retrieved on 07.01.2020.

[27] *Ibidem*, p. 1.

[28] Michael Evans, Daniel McCrery, *"Terrorists Trained in Western Methods Will Leave Few Clues"*, in *London Times*, 12 July 2005. pp.1-3, https://www.thetimes.co.uk/article/terrorists-trained-in-western-methods-will-leave-few-clues-3tgqxdp7q0q, retrieved on 07.01.2020.

[29] Serge Karsavina, *"What is Cyber-Terrorism?"*, in *Computer Crime Research Center,* p. 1, http://www. crime-research.org/analytics/Krasavin/, retrieved on 07.01.2020.

in cyberspace? Some analysts have argued that to fulfil the homeland defence mission, the institutions in the field of security should be given increased authority over private sector critical infrastructure protection. Yet business owners, particularly in the IT sector, contend that this would represent a *"militarisation of cyberspace"* that would create distrust among consumers and shareholders, and could potentially stifle innovation, leading to decreases in profits.

As highlighted, the international community must eliminate a certain amount of ambiguity regarding what constitutes an *"armed attack"* in cyberspace and what the thresholds are for a cyber-attack to be considered an act of war, an incident of national significance, or both. Without clear red lines and specific consequences articulated, deterrence strategies may be incomplete. On the other hand, a lack of red lines and consequences could constitute a form of strategic ambiguity that gives the institutions in the field of security operational manoeuvrability.

Most of defence, public order and national security institutions are supported partially by civilian high technology services and products, most often in the form of communications systems and computer software. A high percentage of military messages "flow" through commercial communications channels, and this reliance creates a vulnerability during conflict or a crisis situation.

CONCLUSIONS

Today, obviously, cyberspace have become another dimension, potentially for both cooperation and conflict. Concern regarding potential damage from cyberterrorism has grown as increasing amounts of economic activity occur online.

Most of defence, public order and national security institutions are supported partially by civilian high technology services and products, most often in the form of communications systems and computer software. A high percentage of military messages *"flow"* through commercial communications channels, and this reliance creates a vulnerability during conflict or a crisis situation. In future conflicts that involve cyberwarfare between states, the distinction between military and civilian targets may be blurred and civilian computer systems may increasingly be seen as viable targets vulnerable to attack by adversaries. Computer networking technology and information systems have also blurred the boundaries between cyberwarfare, cybercrime, and cyberterrorism. Officials in government and industry now say that cybercrime and cyberattack services available for hire from criminal organisations are a growing threat to the states national security as well as to their economy.

New and sophisticated cybercrime tools could operate to allow a state actor or terrorist group to remain unidentified while they direct cyber-attacks through the Internet. It can be concluded that past incidents of conventional terrorism have already been linked with cybercrime, and that computer vulnerabilities may make government and civilian critical infrastructure systems seem attractive as targets for cyberattack. There are indications that suggest possible connections between cybercriminals and terrorist groups that want to damage a state economy or national security interests.

It is clear that terrorist groups are using computers and the Internet to further goals associated with spreading terrorism. This can be seen in the way that extremists are creating and using numerous Internet websites for recruitment and fund-raising activities, and for Jihad training purposes. Several criminals who have recently been convicted of cybercrimes used their technical skills to acquire stolen credit card information in order to finance other conventional terrorist activities.

The states experience difficulties in establishing the strategy for selecting and implementing an appropriate military or legally response after such an attack.

The states experience difficulties in establishing the strategy for selecting and implementing an appropriate military or legally response after such an attack.

Labelling a *"cyberattack"* as *"cybercrime"* or *"cyberterrorism"* is problematic because of the difficulty in determining with certainty the identity, intent, or the political motivations of an attacker.

Suggestions to increase incentives regarding cyber space security may include requiring that all software procured for national agencies should be certified, under the common criteria testing programme, which should also be a mandatory requirement for the software procurement, although the domain analysts point out that the software certification process is lengthy and may interfere with innovation and competitiveness in the global software market.

It may be suggested that the agencies operating national security systems are required to purchase software products from a list of lab-tested and evaluated products in a programme run by the institutions with responsibilities in security.

BIBLIOGRAPHY:

1. ***, *"Convention on Cybercrime"*, in *Council of Europe, European Treaty,* https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId= 0900001680 081561.
2. ***, FBI, *"Terrorism"*, in *What We Investigate*, https://www.fbi.gov/investigate/terrorism.

3. ***, *"International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World"*, in *US Department of State*, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_ strategy_for_cyberspace.pdf.
4. ***, *Law no. 362/2018 on ensuring a common level of security of networks and information systems,* in the *Official Gazette,* Part I no. 21 of 9 January 2019.
5. *** *"National Strategy for Counterterrorism of The United States of America"*, in *The White House*, https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf.
6. ***, *"Significant Cyber Incidents Since 2006"*, in *Centre for Strategic & International Studies*, https://csis-prod.s3.amazonaws.com/s3fs-public/200108_Significant_Cyber_Events_List.pdf?aj4_VlDq2hSan2U8O5mS29Iurq3 G1QKa.
7. ***, *"Tallinn Manual on the International Law Applicable to Cyber Warfare"*, in *The NATO Cooperative Cyber Defence Centre of Excellence*, http://csef.ru/media/articles/3990/ 3990.pdf.
8. ***, United Nations Secretary General, *"Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security"*, *United Nations General Assembly*, https://www.un.org/ga/search/view_ doc.asp?symbol=A/65/201.
9. Barry C. Collin, *"Cyberterrorism"*, in *Institute for Security and Intelligence, 11th Annual International Symposium on Criminal Justice Issues*, https://www.nato.int/structur/ library/bibref/cyberterrorism.pdf.
10. Jonathan Curiel, *"Iraq's Tech-savvy Insurgents Are Finding Supporters and Luring Suicide-bomber Recruits over the Internet"*, in *San Francisco Chronicle*, https://www.sfgate. com/news/article/TERROR-COM-Iraq-s-tech-savvy-insurgents-are-2623261.php.
11. Dorothy Denning, *"Activism, Hacktivism, and Cyberterrorism: The Internet As a Tool for Influencing Foreign Policy"*, in *Nautilus Institute,* Conference on *"The Internet and International Systems",* https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf.
12. Michael Evans, Daniel McGrory, *"Terrorists Trained in Western Methods Will Leave Few Clues"*, in *London Times*, https://www.thetimes.co.uk/article/terrorists-trained-in-western-methods-will-leave-few-clues-3tgqxdp7q0q.
13. Jack Goldsmith, *"Cybersecurity Treaties: A Sceptical View"*, in *Future Challenges in National Security and Law",* http://media.hoover.org/sites/default/files/documents/ Future Challenges_ Goldsmith.pdf.
14. Sarah Gordon, *"Cyberterrorism?"*, in *Symantec White Paper*, https://www.symantec.com/avcenter/reference/cyberterrorism.pdf.

15. Oona A. Hathaway, *"The Law of Cyber-Attack",* in *California Law Review,* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2134932.
16. Jarrett H. Marshall, *"Prosecuting Computer Crimes"*, in *Office of Legal Education Executive Office for United States Attorneys,* https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual. pdf.
17. Olivier Kempf, *"NATO and Cyber Defense"*, in *NDC Research Paper*, https://www.chaire-cyber.fr/IMG/pdf/nato_and_cyberdefense_olivier_kempf_05.2013.pdf.
18. Harold Hongju Koh, *"International Law in Cyberspace"*, in *US Department of State*, *Archived content*, https://2009-2017.state.gov/s/l/releases/remarks/197924.htm.
19. Serge Krasavin, *"What is Cyber-Terrorism?"*, in *Computer Crime Research Center,* http://www. crime-research.org/analytics/Krasavin/.
20. Rollie Lal, *"Terrorists and Organized Crime Join Forces"*, in *The New York Times*, https://www.nytimes.com/2005/05/24/opinion/terrorists-and-organized-crime-join-forces.html.
21. Edward V. Linden, *"Focus on Terrorism"*, in *Nova Science Publishers, Inc*, https://books.google.ro/books?id=wl-Ds42YMDIC&pg=PA30&lpg=PA30&dq=Dan+Verton,+%E2%80%9CA+Definition+of+Cyber-terrorism%E2%80%9D,+Computerworld,+August+11,+2003,+p.6&source=bl&ots=dRkvffLk4i&sig=ACfU3U3wC6ltTKQ2aQM6vL-EkQ2bVKetYg&hl=ro&sa=X&ved=2ahUKEwjBoJaJsYbnAhVil4sKHSzXB8wQ6AEwAHoECAoQAQ#v=onepage&q=Dan%20Verton%2C%20%E2%80%9CA%20Definition%20of%20Cyber-terrorism%E2%80%9D%2C%20Computerworld%2C%20August%2011%2C%202003%2C%20p.6&f=false.
22. Barak Obama, *"Remarks by the President in Year-End Press Conference"*, in *The White House Office of the Press Secretary*, https://obamawhitehouse.archives.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference.
23. Chris Strohm, *"FBI Provides More Proof of North Korea Link to Sony Hack"*, in *Bloomberg*, https://www.bloomberg.com/news/articles/2015-01-07/clapper-warns-of-more-potential-north-korean-hacks-after-sony.
24. Clay Wilson, *"Computer Attack and Cyberterrorism"*, in *Naval History and Heritage Command*, https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/c/computer-attack-cyberterrorism-crs.html.
25. Katharina Ziolkowski, *"Ius ad bellum in Cyberspace – Some Thoughts on the ‹Schmitt-Criteria› for Use of Force"*, in *Legal & Policy Branch NATO CCD COE*, https://ccdcoe.org/uploads/2012/01/5_3_Ziolkowski_IusAdBellumInCyberspace.pdf.