Anda Bologa

To: Professor Charles J. Moxley, Jr.

From: Anda Bologa, LL.M student

Re: Final paper – Contemporary Issues as to Nuclear Weapons and International Law in the Post 9/11 World

STATES' RESPONSIBILITY FOR PROTECTING THEIR NUCLEAR WEAPONS FROM CYBERATTACKS

"Gentlemen, you can't fight in here! This is the War Room!"

Stanley Kubrick, Dr Strangelove or: How I Learned to Stop Worrying and Love the Bomb (1964)

I. INTRODUCTION

Nuclear weapons are dangerous instruments. The devastation of Hiroshima and Nagasaki in 1945 left a horrific mark on the world and since then, the immediate and long-term impacts of testing and usage of nuclear weapons have been widely researched.[1]

While after the end of the World War II, countries that are known to possess nuclear weapons have been reluctant to intentionally use them, there are still a high number of incidents in which nuclear weapons were dangerously close to be used as a result of errors or miscalculations.

Illustratively, Stanislav Petrov, an officer of the Soviet Air Defense Forces prevented in 1983 what is known as perhaps one of the most famous nuclear false alarm incidents that could have resulted in escalation and potentially full-scale nuclear war.[2]

However, since 1983 the internet undeniably and profoundly transformed our world. As stated by the 2003 White House National Security Strategy to Secure Cyberspace,[3] computer networks and information and communication technologies (ICT) constitute the

[1] See Prăvălie R. Nuclear weapons tests and environmental consequences: a global perspective. *Ambio*. 2014;43(6):729-744. doi:10.1007/s13280-014-0491-1, and Humanitarian impacts and risks of use of nuclear weapons, 10th Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, https://www.icrc.org/en/document/humanitarian-impacts-and-risks-use-nuclear-weapons (consulted on 12.10.2021).

[2] Pavel Aksenov, Stanislav Petrov: The man who may have saved the world, https://www.bbc.com/news/world-europe-24280831, (consulted on 12.12.2021).

[3]White House National Security Strategy to Secure Cyberspace, https://georgewbush-whitehouse.archives.gov/pcipb/ (consulted on 11.27.2021).

nerve system of modern society. We have become ever more interconnected – and cyber security incidents more often than not have posed a real threat to a wide area of critical domains, including that of nuclear weapons. For what Petrov had minutes to take a critical decision, nowadays, due to the cyber modernization of the nuclear weapons infrastructure, the military personnel are forced to decide on in fractions of seconds.

The cyber interdependence of the nuclear weapons arsenal poses two major vulnerabilities: increased risks of intentional malicious cyberattacks and the enhanced risk of programming errors due to their growing complexity. It is important to note that given the nature of the nuclear weapons and their increased reliance on computer networks especially in what concerns the nuclear command, control and communication systems, a programming error can prove to have similar catastrophic consequences as an intentional malicious attack. An IBM report underlining that human error has been a contributing factor in over ninety-five percent of all investigated cyber incidents emphasizes the seriousness of this vulnerability.[4]

While aspects of International Law applicability to cyberspace have been previously extensively analyzed, particularly in what concerns offensive operations, such as a state's responsibility for conducting malicious cyberattacks, less attention has been paid to defensive operations, for instance, a state's responsibility to protect its nuclear weapons from cyber threats. Specifically, and to an extent surprisingly, the nexus between the cyber operations and the nuclear weapons is still under researched.

[4] IBM Global Tech. Serv., Ibm Security Services 2014 Cyber Security Intelligence Index 3 (2014), http://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf. (consulted on 11.26.2021)

Thus, this paper aims to fill a gap in discussing the duty a state has under international law to protect its nuclear weapons from cyber threats. To a large extent, this paper will focus on states that both are known to possess nuclear weapons and have nuclear infrastructure ("nuclear power states".)

The first research aim is to examine the source of this obligation and its scope under international law. In order to explore it, I will look at general international law, the specialized international perspective, and finally at obligations states have within international organizations.

This paper asserts that states have an obligation in relation to their citizens and to other states and global community to protect their nuclear weapons from cyber threats. First, by analogy, nuclear power states have a obligation to take appropriate measures, including through legislation and regulations, to prevent, mitigate, and increase their preparedness in the face of disasters, understood as a cyber-attack on their nuclear weapons.

These measures could take the form of national regulations imposing cyber-security standards and building cyber resilience. Second, states have the due diligence obligation to the extent that a state exercises sovereignty over the nuclear weapons within its borders and it shoulders the duty to ensure they are not used to the detriment of other States.

The international law obligations identified by this paper are still in dynamic development and further research is needed in this area. Thereafter, problems for future research are identified, inviting scholars to engage with the applicability of international law to the nexus between cyber threats and nuclear weapons, as a path forward in enhancing the security of nuclear weapons and building cyber resilience.

II. SOURCE OF THE OBLIGATION UNDER INTERNATIONAL LAW

In what concerns an offensive cyberattack, it is a general principle of international law that a breach of an international obligation attributable to a state entails its responsibility,[5] and it has been stated that the law of state responsibility applies fully in cyberspace.[6] Notwithstanding its novelty, existing treaty and customary norms apply to the cyber realm by means of interpretation,[7] their adequacy being confirmed by state practice[8] and doctrine.[9] This means that, as underlined in customary law[10], jurisprudence[11] and doctrine,[12] any illegitimate

[5] *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, ILCR, 53 Sess., UN GAOR, 56th Sess., A/56/49(Vol I)/Corr.4, YILC, 2001

[6] MN Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 1st ed., 2013, 64

[7] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, 1st ed., 2014, 20

[8] *U.S.*Department of Defense, *Strategy for Operating in Cyberspace*, July 2011; Federal Ministry of the Interior, *Cyber Security Strategy for Germany*, February 2011, 15.

[9] MN Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 1st ed., 2013, 64

[10] League of Nations, Conference for the Codification of International Law, *Bases of Discussion for the Conference Drawn Up by the Preparatory Committee*, vol. III, 90.

[11] *Salvador Commercial Company*, UNRIAA, vol.XV (Sales No.66.V.3), 1902, 455

[12] *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, ILCR, 53 Sess., UN GAOR, 56th Sess., A/56/49(Vol I)/Corr.4, YILC, 2001

cyber activity undertaken by a State will entail its responsibility, provided that the evidence pointing at it suffices.[13]

This paper aims to reverse the perspective and examine the responsibility of states that are known to possess nuclear weapons to secure them from cyber threats. Consequently, this section will start by examining the policy considerations in the area, then it will explore the source of this obligation under general international law, the specialized international perspective, and the obligations states have within international organizations.

A. Policy considerations

In the words of an American analytic philosopher, *"To choose a definition is to plead a cause."*[14] The term cyber security is relatively new and started to be increasingly popular after President Barack Obama's address on this subject in 2009.[15]

While the new term has gained acceptance both among the professionals working in the field and the wider public, issues related to definition clarity are still in place. For instance,

[13] *Tallinn Manual*, Rule 6¶6.

[14] Stanford Encyclopedia of Philosophy, "Charles Leslie Stevenson", 2015, https://plato.stanford.edu/entries/stevenson/. (consulted on 11.17.2021).

[15] The White House, "Presidential Proclamation - National Cybersecurity Awareness Month," 2009, https://obamawhitehouse.archives.gov/the-press-office/presidential-proclamation-national-cybersecurity-awareness-month. (consulted on 11.17.2021).

even the syntax of the term across literature and official documents are widely irregular, although the disjoined version appears to dominate.[16]

Unless referring to the primary source material, this paper shall use the disjoint spelling.

In order to discuss cyber security threats, the concept of system vulnerability has to be defined. The academic literature has defined it as: *"the vulnerability of a system is the degree to which that system is unable to cope with selected adverse events."*[17]

When discussing security, one has to distinguish between reality – mathematically calculated risk based on probability and the effectiveness of defense, and perceptions– psychological reactions to it.[18] Indeed, nowadays cyber security is a hot topic. Nevertheless, much like the general concept of security, cyber security is heavily dependent on public perception.

Discussions on the potential catastrophic consequences of cyber-attacks are not new. For instance, UN Secretary General Antonio Gutierrez has declared his absolute conviction that: *" the next war will begin with a massive cyberattack to destroy military capacity... and paralyze basic infrastructure such as the electric networks."*[19]

[16] Schatz, Daniel, Bashroush, Rabih, and Wall, Julie "Towards a More Representative Definition of Cyber Security," Journal of Digital Forensics, Security and Law: (2017) Vol. 12 : No. 2 , Article 8, 55

[17] Sovacool, Benjamin K. Energy Security. (Abingdon, Oxon: Routledge, 2014), 399.

[18] Schneier B. "The Psychology of Security," AFRICACRYPT 2008, LNCS 5023, Springer-Verlag, 2008, 50-79

[19] UN Secretary General Antonio Gutierres, Speech at the University of Lisbon, March 2018, and UN Secretary General Antonio Gutierres Address to the General Assembly, September 2018, https://www.un.org/sg/en/content/sg/speeches/2018-09-25/address-73rd-general-assembly (consulted on 12.12.2021).

By the same token, the 2019 National Intelligence Worldwide Threat Assessment identified cyber threats as the most significant global threat facing the international community, ahead of other threats coming from Russia, China, Iran, and North Korea, or threats of terrorism, weapons of mass destruction, and nuclear proliferation.[20]

There are numerous previous instances when the critical infrastructure of a state was the victim of a cyber attack, most famously in Estonia (2007), Georgia (2008), United Kingdom (2011), Ukraine (2015, 2016, and 2017). In several cases, a connection between inter-state conflicts and the cyber attack can be traced (e.g., Estonia, Georgia).

While what is defined as critical infrastructure varies upon jurisdiction, the U.S. Presidential Policy Directive for Critical Infrastructure Security and Resilience lists Nuclear Reactors, Materials, and Waste Sector as part of US critical infrastructure.[21]

Interestingly, the 2005 EU Green Paper European Programme for Critical Infrastructure[22] defines critical infrastructure based on the cross-border effect, meaning whether the incident on it has a serious impact beyond the territory of a EU Member State where the item is located. More to that, the Green Paper lists the cooperation between EU

[20] Daniel R. Coats, Worldwide Threat Assessment of the US Intelligence Comunity, Senate Select Committee on Intelligence (29 January 2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf (consulted 12.12.2021)

[21] Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/critical-infrastructure-sectors (consulted on 11.23.2021).

[22]Green Paper on a European programme for critical infrastructure protection, https://op.europa.eu/en/publication-detail/-/publication/4e3f9be0-ce1c-4f5c-9fdc-07bdd441fb88/language-en

Member States as an efficient means of addressing the consequences of critical infrastructure located at the border between two states. Naturally, nuclear plants and nuclear weapons fall within this definition.

Recent studies assessing the vulnerability of nuclear weapons to cyberattacks[23] highlighted several major challenges brought by advancements in cyber operations, ranging from the threat of decision makers being manipulated into launching nuclear operations, or the need to take decisions in a significant less amount of time to the process of incorporating new technologies within the nuclear weapons systems, such as Artificial Intelligence (AI) without fully asserting its impact and consequences. This is especially worrisome since according to the Nuclear Threat Initiative (NTI) cyber score index, one third of countries that have nuclear facilities lack basic cyber security.[24]

One solution that is often discussed involves physically disconnecting the nuclear command, control and communication systems networks from the internet, known under the name of "air-gap." However, the example of Stuxnet *("The worm was specifically created to hunt for predetermined network pathways, such as someone using a thumb drive, that would allow the malware to move from an internet-connected system to the critical system on the*

[23]Herbert Lin, Cyber Threats and Nuclear Weapons, Stanford, Stanford University Press, 2021, http://www.sup.org/books/title/?id=34611

[24] Page Stoutland, Erin Dumbacher, Addressing Cyber-Nuclear Security Threats, https://www.nti.org/about/programs-projects/project/addressing-cyber-nuclear-security-threats/ (consulted on 12.12.2021).

other side of the air-gap")[25] has shown that the mere absence of the internet connection does not constitute in itself a viable protective measure.

For instance, the project SHINE (named after SHodanINtelligence Extraction) has unveiled the magnitude of Internet-connected Critical Control Systems[26]. This reveals an alarming fact, namely that most of the system integrators and organizations are not aware of their level of interconnectivity and exposure.[27]

A major impediment for research is represented by the relevant stakeholders' reluctance to share sensitive information related to cyber security incidents. Nonetheless, the importance of cyber security studies will only grow with the continuous digitalization and modernization of the nuclear weapons arsenal.

[25] The Conversation "Can the power grid survive a cyberattack?" https://theconversation.com/can-the-power-grid-survive-a-cyberattack-42295.

[26] Interview with Mr. Robert Radvanovsky, US expert on critical infrastructure protection and assurance, Skype Interview, 30 April 2019.

[27] Fahmida Y. Rashid, "Project SHINE Reveals Magnitude of Internet-connected Critical Control Systems," 2014, SecurityWeek, https://www.securityweek.com/project-shine-reveals-magnitude-internet-connected-critical-control-systems.

B. General International Law

Neither the Treaty on the Prohibition of Nuclear Weapons (TPNW)[28] nor the Treaty on the Non-Proliferation of Nuclear Weapons (NPT)[29] expressly encompass the cyber dimension or provide any obligations that would define a state's responsibility to protect its nuclear weapons from cyberattacks. Thus, one has to search for the source of this obligation under general international law rules.

First, this paper looks at cyberattacks on nuclear weapons through the lenses of natural disasters, then at due diligence understood as a principle of international law applicable to all obligations of conduct.[30]

i. Cyber-attacks on nuclear weapons as natural disasters

A useful analogy in analyzing the responsibility of states to protect their nuclear weapons from cyberattacks would be that of natural disasters. A state owns a responsibility to its own nationals and other individuals within its territory to protect them from consequences

[28]United Nations General Assembly, Treaty on the Prohibition of Nuclear Weapons, A/CONF.229/2017/8 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/209/73/PDF/N1720973.pdf?OpenElement (consulted 11.15.2021)

[29] See Treaty on the Non-Proliferation of Nuclear Weapons (NPT), https://www.un.org/disarmament/wmd/nuclear/npt/text, A/RES/66/33 (2011), A/RES/61/70 (2006), A/RES/56/24 (2001) (consulted on 11.15.2021)

[30] Kulesza, J. (09 Aug. 2016). Due Diligence in International Law, Leiden, The Netherlands: Brill | Nijhoff. Available From: Brill https://doi.org/10.1163/9789004325197 (consulted on 12.13. 2021)

of natural disasters.[31] This obligation derives from the concept of state sovereignty: states are responsible to protect those within their territory and offer a safe environment in which they can pursue their interests.[32]

For instance, the U.N. Charter obligates U.N. Member States *"to take joint and separate action in co-operation with the Organization for the achievement of the purposes set forth in Article 55,"* which promotes respect for human rights and fundamental freedoms.[33]

In 2016 the International Law Commission (ILC) adopted the Draft Articles on the Protection of Persons in the Event of Disasters. According to the draft articles, a disaster is *"a calamitous event or series of events resulting in widespread loss of life, great human suffering and distress, mass displacement, or large-scale material or environmental damage, thereby seriously disrupting the functioning of society".* Consequently, a cyberattack on nuclear weapons could qualify under this definition. Article 7 imposes on states a duty to cooperate: *"In the application of the present draft articles, States shall, as appropriate, cooperate among themselves, with the United Nations, with the components of the Red Cross and Red Crescent Movement, and with other assisting actors."*

Most importantly, Article 9 imposes to states the obligation of disasters risk reduction as follows *"Each State shall reduce the risk of disasters by taking appropriate measures,*

[31] International Law Commission, Draft articles on the protection of persons in the event of disasters, 2016, https://legal.un.org/ilc/texts/instruments/english/draft_articles/6_3_2016.pdf

[32] Thomas H. Lee, The Law of War and the Responsibility to Protect Civilians: A Reinterpretation, 55 HARV. INT'L L.J. 251 (2014); Saira Mohamed, Taking Stock of the Responsibility to Protect, 48 STAN. J. INT'L L. 319 (2012).

[33] U.N.Charter, art.55–56.

including through legislation and regulations, to prevent, mitigate, and prepare for disasters" where *"disaster risk reduction measures include the conduct of risk assessments, the collection and dissemination of risk and past loss information, and the installation and operation of early warning systems."*[34]

By the same token, the 2005 Hyogo Declaration[35] affirms that "*states have the primary responsibility to protect the people and property on their territory from hazards, and thus, it is vital to give high priority to disaster risk reduction in national policy, consistent with their capacities and the resources available to them".*

By the vulnerability of a state's nuclear weapons arsenal the state in case endangers itself and other states and other non-state actors. In this context, nuclear weapons can be regarded as a common concern of the international community, similar to the climate change issue.

This paper argues that by analogy, nuclear power states have a obligation to take appropriate measures, including through legislation and regulations, to prevent, mitigate, and increase their preparedness in the face of disasters, understood as a cyber-attack on their nuclear weapons. These measures could take the form of national regulations imposing cyber-security standards of nuclear weapons arsenal and building its cyber resilience.

[34] Rep. of the Int'l Law Comm'n, 66th Sess., May 5– June 6, July 7– Aug. 8, 2014, U.N. Doc. A/69/10, Ch. V.

[35] World Conference on Disaster Reduction, 18-22 January 2005, Kobe, Hyogo, Japan, Final report of the World Conference on Disaster Reduction (A/CONF.206/6), www.unisdr.org/wcdr (consulted on 11.22.2021).

ii. Due diligence obligation

Cyber security incidents on nuclear weapons can have both cascading effects and consequences on the networks of other states. This does apply to the situation of a nuclear power state being the victim of a cyberattack. Consequently, the failure of nuclear power states to appropriately protect their territory would most certainly affect the fundamental rights of their citizens and inhabitants – and most importantly – their right to life.

While a state's cyber infrastructure is not included in its territory[36] this paper contends that the due diligence obligation referred to in *Corfu* case[37] does apply directly to the extent that a state exercises sovereignty over the nuclear weapons within its borders and it shoulders the duty to ensure they are not used to the detriment of other States[38].

This obligation was previously addressed in *Trail Smelter* case[39] contending that a state *"owes at all times a duty to protect other states against injurious acts by individuals from within their jurisdiction",* and *Island of Palmas* case,[40] noting the duty of every state *"to protect within the territory the rights of other states, in particular their right to integrity and inviolability in peace and in war".*

[36] *Tallinn Manual*, 15.

[37] Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, ¶ 22 (Apr. 9). See also Rorbert P. Barnidge, Jr., The Due Diligence Principle under International Law, 8 INT'L COMM. L. REV. 81 (2006); Riccardo Pisillo-Mazzeschi, The Due Diligence Rule and the Nature of the International Responsibility of States, 35 GERM. Y.B. INT'L L. 9 (1992).

[38] *U.N. Doc. A/70/174*, 22 July 2015,¶13(c).

[39] *Trail Smelter Arbitration (US v Canada)*, 3RIAA, Arb.Trib. 1941, 1911, 1963 .

[40] (Neth. v. U.S.), 2 R.I.A.A. 829, 839 (Perm. Ct. Arb. 1928)

This would be applicable in the case when a state or non-state actor would maliciously direct a cyber-attack to a nuclear weapon of a state and the attack in case would have negative consequences in detriment of other states.

The International Group of Experts that drafted the Tallinn Manual on the International Law of Cyber Warfare ("Tallinn Manual 1"), concluded that a *"State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States."*[41]

Nuclear weapons are in exclusive governmental control, and by analogy, in the digitalization and modernization process undertaken states have the due diligence obligation to secure them from cyber threats. This obligation could take the form of enacting national criminal laws that would prosecute cyberattacks on critical infrastructure (legislative frameworks which would expressly mention nuclear weapons), and conduct comprehensive investigations on the state of cyber preparedness and cyber resilience of their nuclear weapons.

The second edition of the Tallinn Manual on the International Law Applicable to Cyber Operations ("Tallinn Manual 2") lays out a *duty of care* in regards to attacks on dams, dykes, and nuclear electrical generating stations. This *duty of care* refers to a cyber-attack on an installation qualifying as a military objective that contains dangerous forces. While not expressly mentioning nuclear weapons, by analogy it is possible to draw a parallel between the severe consequences on civilian population in the case of an attack on a nuclear electrical generating station and a nuclear weapons facility. In both situations, civilians would face devastating long-lasting effects of such an attack.

[41] Tallinn Manual, (Rule 5).

C. Specialized International Perspective

The Chernobyl nuclear plant accident served as an incentive for states to adopt in 1986 the Convention on Early Notification of a Nuclear Accident[42], which establishes a notification system for nuclear accidents from which a release of radioactive material occurs or is likely to occur and which has resulted or may result in an international transboundary release that could be of radiological safety significance for another State.

This convention requires states to report essential data for assessing the consequences of a nuclear accident, such as its the time, location, and nature. Article 1 of the Convention makes reporting mandatory for any nuclear accident involving a list of facilities and activities, such as any nuclear reactor and nuclear waste material. Unfortunately, the convention does not impose specific and mandatory requirements on state parties.

The 1997 Vienna Convention on Civil Liability for Nuclear Damage provides a liability regime of the operator of a nuclear installation against damage from certain peaceful uses of nuclear energy. The Convention provides for *absolute* and *strict* liability; hence the injured parties do not have to prove the fault or the negligence of the nuclear operator.[43]

The Convention is designed to ensure that all Contracting Parties have laws and regulations in place conforming to the legal regime for civil liability for nuclear damage provided for in the Convention.

---

[42] Convention on Early Notification of a Nuclear Accident, NFCIRC/335 https://www.iaea.org/sites/default/files/infcirc335.pdf

[43] Vienna Convention on Civil Liability for Nuclear Damage, https://www.iaea.org/topics/nuclear-liability-conventions/vienna-convention-on-civil-liability-for-nuclear-damage (consulted 12.10.2021).

The legal regime provided for in the Convention is based on the following general principles:

- *"exclusive liability of the operator of the nuclear installation concerned;*
- *"absolute" or "strict" liability, so that the injured party is not required to prove fault or negligence on the part of the operator;*
- *minimum amount of liability;*
- *obligation for the operator to cover liability through insurance or other financial security;*
- *limitation of liability in time;*
- *equal treatment of victims, irrespective of nationality, domicile or residence, provided that damage is suffered within the geographical scope of the Convention;*
- *exclusive jurisdictional competence of the courts of the Contracting Party in whose territory the incident occurs or, in case of an incident outside the territories of Contracting Parties (in the course of transport of nuclear material), of the Contracting Party in whose territory the liable operator's installation is situated);*
- *recognition and enforcement of final judgements rendered by the competent court in all Contracting Parties."*[44]

The Convention on Assistance in the event of a nuclear accident (1986) sets out an international framework for co-operation among States Parties and with the IAEA to facilitate prompt assistance and support in the event of nuclear accidents or radiological emergencies.

[44] Vienna Convention on Civil Liability for Nuclear Damage, https://www.iaea.org/topics/nuclear-liability-conventions/vienna-convention-on-civil-liability-for-nuclear-damage (consulted 12.10.2021).

It requires States to notify the IAEA of their available experts, equipment, and materials for providing assistance. In case of a request, each State Party decides whether it can render the requested assistance as well as its scope and terms. Consequently, in case of a cyber attack on nuclear weapons arsenal, states parties to the Convention on Assistance in the event of a nuclear accident would have to render assistance to the affected state, should it ask for cooperation, experts, or other assistance.

European Convention on Cybercrime criminalizes cyber-attacks and imposes to states the duty to prevent territories from being used by non-state actors to conduct cyber-attacks.[45] This convention was ratified by the members of the Council of Europe, but also by the United States, Australia, Canada, and Japan, and several other states.

Article 7 of the Convention states that *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches."*

Article 11 states that *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an*

[45] Convention on Cybercrime, Council of Europe, Nov. 23, 2001, 41 I.L.M. 282, 2296 U.N.T.S. 167.

attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c of this Convention."

Article 13 states that *"Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions."*

Therefore, states parties of the European Convention on Cybercrime have the obligation to set in place a regulatory framework that would criminalize cyber attacks. By interpretation, these states may have the obligation to protect their territory for being used to conduct cyber attacks. In case of nuclear power states, this would encompass the nuclear weapons arsenal.

D. International Organizations

i. United Nations

Within the United Nations, issues of disarmament and international security fall under the First Committee agenda, in accordance with the United Nations Charter. The 2015 report by the United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (GGE), adopted by consensus by the UN General Assembly,[46] indicates that states *"should not knowingly allow their territory to be used for internationally wrongful acts using ICTs."*

The report reaffirmed that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment.

Relevant provisions for nuclear power states would be the work of the UN Open Ended Working Group (OEWG) of States which concluded that ICT activity contrary to obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public, could pose a threat not only to security but also to State sovereignty, as well as economic development and livelihoods, and ultimately the safety and wellbeing of individuals.[47]

[46] GA Res. 70/237, 30 December 2015, §§ 1–2(a).

[47] A/AC.290/2021/CRP.2, Open-ended working group on developments in the field of information and telecommunications in the context of international security

The U.N. General Assembly has also called for the criminalization of cyber attacks,[48] prevention of allowing safe havens to launch cyber attacks,[49] and cooperation in the investigation and prosecution of international cyber attacks.[50] The General Assembly and some states have also labeled cyber attacks as a threat to international peace and security.[51]

While non-binding, the *Code of Conduct for Information Security* submitted in 2015 to the UNGA[52], reaffirms, *inter alia*, the prohibition on carrying out activities that run counter to the task of maintaining peace and security[53], which is resident in customary law[54], as well as codified in Article 2(4) of the *UN Charter*. Whether cyber operations on nuclear weapons qualify as use of force depends on the measurement of their 'scale and effects'[55]. This view is widely shared among jurists[56], and has been embraced by USA[57] and Russia[58], among others.

[48] G.A. Res. 45/121, ¶ 3 (Dec. 14, 1990).

[49] G.A. Res. 55/63, ¶ 1 (Jan. 22, 2001).

[50] G.A. Res. 55/63, ¶ 1 (Jan. 22, 2001).

[51] Dep'tof Homeland Sec., The Nat'l Strategy To Secure Cyberspace 49– 52 (2003), http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy. pdf; G.A. Res. 45/121,

[52] *U.N. Doc. A/69/723*, 13 January 2015.

[53] *Ibid.*,¶2.

[54] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ICJ Reports 1996,¶39;

[55] *Tallin Manual*, Rule 11.

[56] *Roscini*, 44; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, Cambridge University Press, 2012, 74.

[57] *U.S.*Department of Defense, *An Assessment of International Legal Issues in Information Operations*, May 1999, 18.

[58] *U.N. Doc. A/C.1/53/3*, 30 September 1998.

ii. International Atomic Energy Agency (IAEA)

The Statute of the International Atomic Energy Agency (IAEA)[59] was approved on 23 October 1956 by the Conference on the Statute of the International Atomic Energy Agency, which was held at the Headquarters of the United Nations and came into force on 29 July 1957. The International Atomic Energy Agency, which provides countries with assistance and training in this area, does not encompass any obligations as to the thesis of this paper.

III. CONCLUSION

Relatively consistent and stable for over a century, the nuclear weapons arsenal is going now through significant digital transformations. The implementation of ITC, along with other digital developments has stirred the overall interconnectivity. The digital transformation gives rise to new benefits but also opens the door for cyber disruptions.

The present paper is an attempt to look at the nexus between cyber security and the nuclear weapons. In particular, it looked at the international liability regime states have to protect their nuclear weapons from cyber threats. Additionally, it looked at policy considerations at the nexus between cyber security and nuclear weapons, especially in what concerns vulnerabilities that states fail to address adequately.

[59]The Statute of the International Atomic Energy Agency, https://www.iaea.org/sites/default/files/statute.pdf

The research conducted aimed to answer the question: is there a liability regime under international law that would mandate states to protect their nuclear weapons from cyber threats? As can be seen from this analysis, the research has concluded that the international legal framework does not encompass a direct obligation that would mandate states to protect their nuclear weapons from cyber-attacks.

Two significant issues stand as an obstacle to establish and thereby enforce a legal framework targeting a cyber-attack on nuclear weapons. First, the predicament of detecting a cyber attack which is often uncovered only a significant time after the initial incursion and the challenging rules of attribution. Second, the underreporting of the cyber incidents, in part determined by national security concerns and international mistrust.

Moreover, in what concerns the operational aspects, given the sensitivity of the information and its relevance for national security, not many resources and data are openly available to the public. Therefore, at the moment, a suitable international legal framework that would enhance cyber resilience becomes hard to develop, and to some extent impossible.

Encompassing into itself the element of novelty, the cyber protection of the nuclear weapons should receive more scholar attention. A large-scale cyber attack, including one targeting the nuclear weapons arsenal is no longer a *"black swan"* event: experts have been warning that it is only a matter of time. Policy makers and legislators should bear in mind that any substantial adverse event, as for instance a massive cyber attack, often brings as a consequence an overreaction response. For instance, after the 9/11 terrorist attack, serious privacy concerns have been raised as a critique of the policies implemented. Arriving at a

consensus regarding the international law obligations that states have to protect their nuclear weapons before an attack would reduce this overreaction factor.

In the words Frank Umbach, a cyber security expert: *"The European Energy Policy was set up after the Russian-Ukrainian gas crisis. The Yugoslav conflict has triggered the European Foreign Security policy.*

It was always an external event, crisis or conflict happening which was the triggering a stronger response on our side. This is how democracies work: politicians do not like to be guided by worse case scenarios, they very much diplomatically like preventive diplomacy, but preventive diplomacies cost much in terms of financing. Despite the progress, we have, in respect to detecting capabilities we probably have to experience a significant cyber attack in order to come up with a more effective response."[60]

Although an international regulatory regime for the states or non-state actors who have initiated the cyber threat is more robust, this paper contends that there are specific obligations that target the state directly affected by the cyber security incidents.

In order to be able to meet these obligations, states should first and foremost adopt national liability regimes criminalizing cyber attacks on nuclear weapons. Next, states should invest both in infrastructure and in human resources in order to assess the seriousness of a cyber threat targeting the nuclear weapons at a early stage. Lastly, states should cooperate in order to

[60] Interview with Dr. Frank Umbach, Research Director, (European Centre for Energy and Resource Security, King's College, London and international consultant on international energy security, geopolitical risks, cyber security and critical energy infrastructure protection; Visiting professor, European Interdisciplinary Studies Department, College of Europe in Natolin), Warsaw, 5 April 2019.

coordinate their efforts in fighting the cascade effect that a cyber-attack on nuclear weapons would have. At the same time, cooperation in mitigation of harmful effects could be accomplished through channels of communication with other state and non-state actors.

For the purpose of this research, various academic materials have been consulted, in the majority of them international conventions, policy reports, comparative analyses, and academic articles. Another resource consisted of interviews with international law experts, academia representatives, and cyber security experts. However, the research resources available were limited, given the novelty of the issue.

In conclusion, digitalization is bringing a rollercoaster of changes, including in what concerns the nuclear weapons arsenal. Many of these changes bring security benefits, especially in terms of using digitalization to enhance the potential of control and command of nuclear weapons. But with those benefits come risks – and cyber security risks, while often difficult to see and understand, are probably the most important.