COMMINGLED NUCLEAR AND CYBER FACILITIES: OBLIGATIONS OF STATES TO TAKE PRECAUTIONS AGAINST THE EFFECTS OF A CYBERATTACK

TRASON LASLEY*

ABSTRACT

In June 2010, a unique virus was broadly introduced to the world. This virus didn't affect all it came in contact with; it only infected hosts that met specific requirements and was never meant to leave a particular host. With that said, the virus escaped and infections were found worldwide. Luckily, no humans were ever affected by this virus directly; instead, it was a cyberweapon, later coined Stuxnet, that was developed to target Iranian nuclear facilities.

States in a time of war have a duty under the law of armed conflict not to attack installations containing dangerous forces, such as nuclear-generating stations, because of the harm they would cause to civilians. However, when states combine nuclear development facilities and the development of malicious cyberwarfare weapons within the same cyberinfrastructure, they forfeit protections under the law of armed conflict that would prohibit states from attacking said nuclear facilities. Because of this, states that combine such industries inherit a duty, under Article 58 of Additional Protocol I, to their civilian population to put in place safeguards to protect nuclear facilities from being victims of cyberwarfare and, therefore, protect their citizens from the effects of such attacks.

* J. Reuben Clark Law School, BYU, Juris Doctor, 2024. Special thanks to Professor Eric Talbot Jensen of J. Reuben Clark Law School, who provided excellent guidance and encouragement throughout the writing, editing, and publishing process and for being a person I can always come to for advice. Thank you to Abbey Lasley, my lovely wife, and my three boys for their continued love and support. I could not do anything without them. Finally, thank you to the Wisconsin International Law Journal staff for their help throughout the publication process, primarily through essential edits and revisions.

https://doi.org/10.59015/wilj.KLCM3237

https://doi.org/10.59015/wilj.KLCM3237

INTRODUCTION

In June 2010, a unique virus was broadly introduced to the world.[1] Yet it wasn't until July 15, 2010, that a widely reputable journalist first reported the virus.[2] A lab later estimated that the virus started spreading around March or April of 2010, with the first variants likely appearing in June 2009.[3] Researchers, however, have since uncovered a version of the virus that was used to attack Iran in November 2007, with an early variant that is thought to have been developed in 2005.[4] A second variant, which included substantial improvements, appeared in March 2010.[5] Despite this, the creators likely feared the second variant was not spreading fast enough and a third variant, with minor improvements, arose in April 2010.[6] This virus didn't affect all it came in contact with; it only infected hosts that met specific requirements and was never meant to leave its intended target.[7] With that said, the virus got out and infections were found worldwide. 58.8 percent of the infected were in Iran, 18.2 percent in Indonesia, and 8.3 percent in India, with a small percentage infected in Azerbaijan, the United States, Pakistan, and other countries.[8]

Luckily, no humans were ever infected by this virus; instead, it was a computer virus that was meant to target Iranian nuclear development.[9] Unlike most malware, this cyberweapon, coined Stuxnet,

---

1 Brian Krebs, *Experts Warn of New Windows Shortcut Flaw*, KREBS ON SEC. (July 16, 2010, 7:49 PM), https://krebsonsecurity.com/2010/07/experts-warn-of-new-windows-shortcut-flaw/ [https://perma.cc/VFR2-Y4NM].

2 Michael Joseph Gross, *A Declaration of Cyber-War*, VANITY FAIR (Mar. 2, 2011), https://www.vanityfair.com/news/2011/03/stuxnet-201104 [https://perma.cc/BGT8-24CQ].

3 Aleks, *Myrtus and Guava: The Epidemic, the Trends, the Numbers*, SECURELIST (Sept. 26, 2010, 7:28 PM), https://web.archive.org/web/20110101113112/http://www.securelist.com/en/blog/325/Myrtus_and_Guava_the_epidemic_the_trends_the_numbers [https://perma.cc/24SL-N2JP]; Gross, *supra* note 2.

4 Jim Finkle, *Researchers Say Stuxnet Was Deployed Against Iran in 2007*, REUTERS (Feb. 26, 2013, 4:00 PM), https://www.reuters.com/article/us-cyberwar-stuxnet-idUSBRE91P0PP20130226/ [https://perma.cc/DK9S-64WA].

5 Gross, *supra* note 2.

6 *Id.*

7 William J. Broad et al., *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES (Jan. 15, 2011), https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&ref=general&src=me&pagewanted=all [https://perma.cc/ZXN6-79DM].

8 Jarrad Shearer, *W32.Stuxnet*, SYMANTEC (Sept. 17, 2010, 8:53 AM) https://web.archive.org/web/20120104215049/http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99 [https://perma.cc/H85C-32XS].

9 *See* Broad, *supra* note 7.

https://doi.org/10.59015/wilj.KLCM3237

only harmed computers and networks with specific network configuration requirements.[10] It also contained specific safeguards that prevented each infected device from spreading the virus to more than three other computers and another that caused it to erase itself on a specific date in 2012.[11] Despite these safeguards, the malware still inadvertently spread further than originally intended.[12]

Experts believe that Stuxnet was the largest, and possibly the most costly, development in the history of malware,[13] requiring many months or years to write the code.[14] *The Guardian*, the *BBC*, and *The New York Times* all reported that those studying the malware believed that Stuxnet was so complex that only a nation-state could produce such a weapon.[15] Many believe that the origins of the attack were Israeli; however, they were most likely backed by a much larger Western ally.[16]

Ralph Langner, a German cybersecurity researcher, claimed that "Stuxnet is a 100-percent-directed cyber-attack aimed at destroying an industrial process in the physical world."[17] He also claimed that it was "not about espionage, as some have said. This is a 100 percent sabotage attack."[18] On November 23, 2010, Natanz nuclear facilities announced that it had ceased operations several times because of a series of major technical problems.[19] Statistics published by the International Atomic Energy Association indicated that the number of enrichment centrifuges that were operational in Iran declined by 15 percent following the release

---

[10] *See* Gross, *supra* note 2.

[11] *Id.*

[12] *See generally* Aleks, *supra* note 3; Gross, *supra* note 2.

[13] Gross, *supra* note 2.

[14] Kim Zetter, *Blockbuster Worm Aimed for Infrastructure, but No Proof Iran Nukes Were Target*, WIRED (Sept. 23, 2010, 3:57 PM), https://www.wired.com/2010/09/stuxnet-2/ [https://perma.cc/7MMK-KTJY].

[15] *See* Jonathan Fildes, *Stuxnet Worm 'Targeted High-Value Iranian Assets*,*'* BBC (Sept. 23, 2010), https://www.bbc.com/news/technology-11388018 [https://perma.cc/V4PY-9ZPK]; *see* Josh Halliday, *Stuxnet Worm is the 'Work of a National Government Agency*,*'* GUARDIAN (Sept. 24, 2010, 10:35 AM), https://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency [https://perma.cc/27ZH-CBZU]; *see* John Markoff, *A Silent Attack, but Not a Subtle One*, N.Y. TIMES (Sept. 26, 2010), https://www.nytimes.com/2010/09/27/technology/27virus.html [https://perma.cc/6KUM-Z3DX].

[16] Gross, *supra* note 2.

[17] Arthur Bright, *Clues Emerge About Genesis of Stuxnet Worm*, CHRISTIAN SCI. MONITOR (Oct. 1, 2010, 9:05 AM), https://www.csmonitor.com/World/terrorism-security/2010/1001/Clues-emerge-about-genesis-of-Stuxnet-worm [https://perma.cc/8VXM-9SS4].

[18] *Id.*

[19] Yossi Melman, *Iran Pauses Uranium Enrichment at Natanz Nuclear Plant*, HAARETZ (Nov. 23, 2010), https://www.haaretz.com/2010-11-23/ty-article/iran-pauses-uranium-enrichment-at-natanz-nuclear-plant/0000017f-db29-d856-a37f-ffe9817b0000 [https://perma.cc/MLL7-3NRD].

https://doi.org/10.59015/wilj.KLCM3237

of Stuxnet.[20] In addition, a serious nuclear accident occurred in the first half of 2009, possibly linked to Stuxnet.[21] The Institute for Science and International Security suggested in a report from December 2010 that Stuxnet is a reasonable explanation for the apparent damage at the Natanz facilities.[22] The authors of the report indicated that:

> the attacks seem designed to force a change in the centrifuge's rotor speed, first raising the speed and then lowering it. . . . If its goal was to quickly destroy all the centrifuges in the FEP [Fuel Enrichment Plant], Stuxnet failed. But if the goal was to destroy a more limited number of centrifuges and set back Iran's progress in operating the FEP, while making detection difficult, it may have succeeded, at least temporarily.[23]

For Natanz the destruction of the nuclear facilities was minimal, with little damage and no reported harm to human life.[24] Outside of one serious accident that may or may not have been caused by the Stuxnet malware, no other damage was done except for slowing down the production of the nuclear facilities.[25] Yet, it is not far-fetched to envision a situation in which cyber means could cause more catastrophic harm to a nuclear facility, damaging not only the production of the facility but also the workers at the plant, civilians living nearby, and the environment, making the location uninhabitable for years. Such a catastrophic disaster could easily be caused by a targeted cyberattack like Stuxnet.

A situation like the one mentioned above is even more likely in times of war, especially where nuclear facilities provide essential power to opposing parties. For example, this situation has been shown in the ongoing—at the time of this Article—war between Russia and Ukraine,

---

[20] *See* DAVID ALBRIGHT & JACQUELINE SHIRE, IAEA REPORT ON IRAN: FORDOW ENRICHMENT PLANT AT "ADVANCED STAGE OF CONSTRUCTION;" DECLINE IN NUMBER P1 CENTRIFUGES ENRICHING BUT P1 CENTRIFUGE EFFICIENCY INCREASES; DISCOVERY OF PREVIOUSLY UNKNOWN STOCK OF HEAVY WATER 1 (2009).

[21] *See* Julian Assange, *Serious Nuclear Accident May Lay Behind Iranian Nuke Chief's Mystery Resignation*, WIKILEAKS (July 16, 2009), https://web.archive.org/web/20101230121529/http://mirror.wikileaks.info/wiki/Serious_nuclear_accident_may_lay_behind_Iranian_nuke_chief's_mystery_resignation/ [https://perma.cc/994Z-CAV3]; T.S., *A Cyber-Missile Aimed at Iran?*, ECONOMIST (Sept. 24, 2010), https://www.economist.com/babbage/2010/09/24/a-cyber-missile-aimed-at-iran [https://perma.cc/3RPN-YBD7].

[22] *See* DAVID ALBRIGHT ET AL., DID STUXNET TAKE OUT 1,000 CENTRIFUGES AT THE NATANZ ENRICHMENT PLANT? 3–5 (2010).

[23] *Id.* at 6–7.

[24] ALEXANDRA VAN DINE, AFTER STUXNET: ACKNOWLEDGING THE CYBER THREAT TO NUCLEAR FACILITIES 111 (2017).

[25] *See* Assange, *supra* note 21; ALBRIGHT ET AL., *supra* note 22, at 7.

https://doi.org/10.59015/wilj.KLCM3237

where there have been attacks on nuclear plants in Ukraine (although not cyberattacks).[26] According to Rule 56 of Additional Protocol I of the Geneva Conventions, nuclear facilities "shall not be made the object of attack, even where these objects are military objectives if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population."[27] This is true with tangible weapons, like missiles or other artillery, and cyberweapons.[28]

On the other hand, the destruction of military weaponry has always been an important part of military operations.[29] Therefore, in the international law of armed conflict, states are allowed to attack and destroy military infrastructure under military necessity.[30] This is also true for locations that develop weapons and even cyberweapons.[31] What then happens to the protection of nuclear facilities when states commingle them with cyberweapons facilities?

States in a time of war have a duty under the law of armed conflict not to attack installations containing *dangerous forces*, such as dams, dykes, and nuclear-generating stations, because of the harm they would cause to civilians.[32] However, when states combine nuclear-development facilities and facilities that develop malicious cyberwarfare weapons within the same cyberinfrastructure, they forfeit protections under the law of armed conflict that would prohibit states from attacking said nuclear

---

[26] *See* Mark Hibbs, *What Comes After Russia's Attack on a Ukrainian Nuclear Power Station?*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Mar. 17, 2022), https://carnegieendowment.org/2022/03/17/what-comes-after-russia-s-attack-on-ukrainian-nuclear-power-station-pub-86667 [https://perma.cc/33LC-YFEB]; *see Zaporizhzhia Nuclear Plant Reports Shelling by Ukraine Army*, REUTERS (Mar. 14, 2024, 2:53 AM), https://www.reuters.com/world/europe/russia-controlled-zaporizhzhia-nuclear-plant-says-was-shelled-by-ukraine-2024-03-14/ [https://perma.cc/D9UN-GG55].

[27] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 56(1), June 8, 1977, 1125 U.N.T.S. 28 [hereinafter Additional Protocol I].

[28] *Cyber Warfare: Does International Humanitarian Law Apply?*, INT'L COMM. OF THE RED CROSS (Feb. 25, 2021), https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law [https://perma.cc/DG5S-LGMX].

[29] *See generally* Additional Protocol I, *supra* note 27.

[30] *See* GENERAL ORDERS NO. 100, INSTRUCTIONS FOR THE GOVERNMENT OF ARMIES OF THE UNITED STATES IN THE FIELD (1863), *reprinted in* 3 THE WAR OF THE REBELLION: A COMPILATION OF THE OFFICIAL RECORDS OF THE UNION AND CONFEDERATE ARMIES 148, 150 (Gov't Printing Off., Ser. No. 3, 1988).

[31] *See generally Military Necessity*, INT'L COMM. OF THE RED CROSS, https://casebook.icrc.org/a_to_z/glossary/military-necessity [https://perma.cc/FSN2-BC7L] (last visited Mar. 15, 2024).

[32] Additional Protocol I, *supra* note 27, at 28.

https://doi.org/10.59015/wilj.KLCM3237

facilities.[33] Because of this, states that combine such industries inherit a duty, under Article 58 of Additional Protocol I, to their civilian population to put in place safeguards, like the separation of servers and firewalls, in order to protect nuclear facilities from cyberwarfare and thus protect their citizens from the effects of such attacks.[34]

The aim of this Article is to determine the obligations of states under the law of armed conflict to protect nuclear facilities from cyberattacks when they have commingled these facilities with cyberweapon development facilities. First, Part I outlines the legal framework of the law of armed conflict. Next, Part II outlines the implications of combining nuclear and cyberweapon development facilities. Part III outlines the duties of attacking states to protect civilians in their attack. Part IV outlines the duty of states, under Article 58, to protect nuclear facilities from cyberattacks when they commingle such facilities with cyberweapon development, using the United States policy on human shields as an analogous framework. Last, Part V outlines the specific precautions states should take in order to comply with their Article 58 obligations.

I. LEGAL FRAMEWORK

First, it is prudent to understand the current international law that governs conflicts during times of war in order to fully understand the implications of states integrating nuclear facilities with cyberweapon development facilities. This Part will summarize the law of armed conflict, then go into more detail about the specific articles from Additional Protocol I of the Geneva Conventions that are integral to cyberwarfare and nuclear facilities.

A. THE LAW OF ARMED CONFLICT

The law of armed conflict is a set of rules and principles that regulate the conduct of armed conflicts.[35] Its primary goal is to mitigate the effects of armed conflict and protect individuals who are not or are no longer participating in the hostilities.[36] Obligations under the law of armed

---

[33] *See id.* at 26.

[34] *See id.* at 29 (stating that parties must take necessary precautions to protect civilians).

[35] *Id.* at 7.

[36] *See id.* at 29.

https://doi.org/10.59015/wilj.KLCM3237

conflict include that parties distinguish between combatants and civilians (including between military objectives and civilian objects) and that the use of force be proportionate to the military objective, to speak to only a small part of the law of armed conflict.[37] In short, the law of armed conflict is designed to strike a balance between military necessity and humanitarian considerations, aiming to minimize the suffering and protect the rights of those affected by armed conflicts.[38]

For the purpose of this Article, some liberties will be taken with some of the initial analysis usually needed to take place in determining the appropriate international law that applies. For starters, this Article will assume an armed conflict exists when analyzing the implications of combining nuclear and cyberwarfare facilities. In addition, it will assume that the applicable law falls under an international armed conflict and not a non-international one; therefore, the appropriate law will apply. With that being said, this Article will now focus on the specific articles of Additional Protocol I of the Geneva Conventions.

1. Additional Protocol I

Additional Protocol I to the Geneva Conventions is an international treaty that supplements and enhances the protection afforded by the four Geneva Conventions of 1949.[39] It was adopted on June 8, 1977, and entered into force on December 7, 1978.[40] The protocol essentially responded to the evolving nature of armed conflicts and aimed to strengthen the legal framework for protecting victims in international armed conflicts.[41]

The development of Additional Protocol I took place against the backdrop of increasing concerns about the conduct of armed conflicts and the need for more comprehensive legal provisions to protect civilian

---

[37] *See id.* at 23.

[38] *See* John Cherry & Michael Rizzotti, *Understanding Self-Defense and the Law of Armed Conflict*, LIEBER INST. W. POINT (Mar. 9, 2021), https://lieber.westpoint.edu/understanding-self-defense-law-armed-conflict/ [https://perma.cc/4QX4-KNRP].

[39] *See* AM. RED CROSS, SUMMARY OF THE GENEVA CONVENTIONS OF 1949 AND THEIR ADDITIONAL PROTOCOLS 1 (2011), https://www.redcross.org/content/dam/redcross/atg/PDF_s/International_Services/International_Humanitarian_Law/IHL_SummaryGenevaConv.pdf [https://perma.cc/T5LQ-LQJU].

[40] Judith Gardam, *Introductory Note* to PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 (2021), https://legal.un.org/avl/ha/pagc/pagc.html [https://perma.cc/9KLX-2U6U].

[41] *Id.*

https://doi.org/10.59015/wilj.KLCM3237

populations during armed conflict.[42] The 1949 Geneva Conventions—which primarily addressed the protection of wounded, sick, and shipwrecked military personnel, prisoners of war, and civilians in times of war—were seen as inadequate in certain respects, given the changing nature of armed conflicts.[43]

For brevity, it is prudent to say here that Additional Protocol I extends the protections provided by the 1949 Geneva Conventions to victims of international armed conflicts.[44] It sets out detailed rules regarding the conduct of hostilities, the treatment of civilians, and the protection of certain categories of individuals during armed conflicts.[45]

While Additional Protocol I has gained widespread acceptance internationally, with many of the provisions being seen by some states as customary international law, not all states are party to the treaty and some states have signed the treaty but not ratified it – like the United States.[46] Others continue to have concerns about some provisions and maintain reservations.[47] Nevertheless, Additional Protocol I is seen as a significant instrument that shapes the legal framework for the protection of victims in international armed conflicts, in addition to influencing the development of customary international humanitarian law.[48]

Not all of the Articles in the Additional Protocol I apply to the topic of this Article, and for that reason, this Article will not elaborate on the Articles that are not crucial to the commingling of nuclear and cyberweapon development facilities. The applicable Articles, and the ones that are needed to understand the issues at hand, are Articles 51, 52, 56, 57, and 58. Next, this Article will briefly explain each of these Articles to lay a foundation before analyzing the issues more specifically.

a. Article 51

In general, Article 51 of Additional Protocol I to the Geneva Conventions addresses the general protection of civilians during armed

---

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] *See Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977*, IHL DATABASES.

[47] *Id.*

[48] *See Legal Framework of Genocide and Related Crimes*, UNITED NATIONS, https://www.un.org/en/genocide-prevention/legal-framework [https://perma.cc/Y4CJ-AY5C] (last visited Mar. 15, 2024).

https://doi.org/10.59015/wilj.KLCM3237

conflicts.[49] It outlines the fundamental principles and rules governing the conduct of hostilities to minimize harm to civilians and civilian objects when civilians do not take part in hostilities.[50]

Article 51(1) makes a general declaration that civilians are entitled to protections against dangers that arise from military operations, declaring that the following rules, "which are additional to other applicable rules of international law," must be observed by states in all circumstances.[51] It affirms the principle that civilians shall enjoy general protection against dangers arising from military operations.[52]

Article 51(7) is a warning that states are not to use the presence of civilian populations, or even a single civilian, to prevent certain points or areas from being objects of military operations.[53] This specifically applies to efforts by states "to shield military objectives from attacks or to shield, favor or impede military operations."[54] Civilian populations can neither be directed to move nor used in their natural movement according to this paragraph.[55]

Commentary from the International Committee of the Red Cross (ICRC) ties this Article to Article 12(4) of Additional Protocol I.[56] Article 12(4) prohibits medical units from being used to shield military operations.[57] For that reason, the protections within this Article appear to apply beyond just civilian populations and could apply to civilian objects that are being used to shield military objectives.

In summary, Article 51 of Additional Protocol I establishes specific protections for civilians during times of conflict as long as they do not take part in the hostilities.[58] In particular, this Article is mainly concerned with paragraph seven of the Article, which prohibits civilians from being used as shields to block attacks on military objectives.[59] As explained further below, this applies to using nuclear facilities as a shield to protect the development of cyberweapons from cyberattacks.

---

[49] *See* Additional Protocol I, *supra* note 27, at 26.

[50] *See id.*

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] *Id.*

[55] *Id.*

[56] *See* CLAUDE PILLOUD ET AL., COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 165 (Yves Sandoz et al. eds., 1987).

[57] *Id.*

[58] *See* Additional Protocol I, *supra* note 27, at 26.

[59] *See id.*

https://doi.org/10.59015/wilj.KLCM3237

b. Article 52

Article 52 of Additional Protocol I to the Geneva Conventions generally addresses the principle of distinction in the conduct of hostilities.[60] This Article underscores the importance of distinguishing between civilian objects and military objectives during armed conflict.[61] This principle of distinction is a core tenet of the law of armed conflict and aims to minimize harm to civilians and civilian infrastructure.[62]

Article 52(1) explicitly prohibits attacks against civilians, civilian populations, or civilian objects. Any attack that treats civilians or civilian objects as the primary target is considered a violation of this provision.[63]

Article 52(2) defines civilian objects as any objects that are not military objectives.[64] On the other hand, military objectives are those that "by their nature, location, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization offers a definite military advantage."[65]

The distinction between military and civilian is important because it governs what can and cannot be targeted by opposing military forces.[66] If the object is military, then it can be targeted if it offers a definite military advantage.[67] On the other hand, if it is not military, then it is civilian, and such objects are not to be targeted.[68] In the case of nuclear facilities, they are civilian and cannot be targeted.[69] In contrast, the cyberwarfare weapons development facilities, by their purpose, make an effective contribution to military action and, therefore, can be targeted when they offer a definite military advantage.[70] But the main question here is what happens when these two objects are commingled into one, which will be discussed in greater detail later.

---

60 *See id.* at 27.
61 *See id.*
62 *Id.*
63 *Id.*
64 *Id.*
65 *Id.*
66 *Id.*
67 *Id.*
68 *Id.*
69 *Id.*
70 *Id.*

https://doi.org/10.59015/wilj.KLCM3237

c. Article 56

Article 56 of Additional Protocol I to the Geneva Conventions addresses the protection of works and installations containing dangerous forces during armed conflicts.[71] This Article is essential to the law of armed conflict, which aims to safeguard certain essential civilian infrastructures that could cause great destruction and to prevent unnecessary harm to civilians during hostilities.[72]

To be specific, Article 56(1) outlines what installations contain dangerous forces under international law.[73] It provides protection to installations such as dams, dykes, and nuclear electrical generating stations from being objects of attack.[74] This protection is granted even if these installations are being used for military purposes and contribute to military action, as long as an attack "may cause the release of dangerous forces and consequent severe losses among the civilian population."[75] In addition, if there are other military objectives located at or near the vicinity of one of these installations, these objectives cannot be made the object of attack if an attack on that objective would also release dangerous forces from the installation and lead to severe losses for the civilian population.[76]

Article 56(3) provides that, in all cases, even when works and installations are protected, the civilian population "shall remain entitled to all the protections accorded to them by international law, including the protection of the precautionary measures provided for in Article 57."[77] This means that all practical precautions must be taken to ensure that the dangerous forces of such installations are not released on civilians.[78]

Article 56(5) obligates state parties to a conflict to avoid locating any possible military objectives in the vicinity of installations that contain dangerous forces.[79] This particular provision was only added in 1973.[80] It was noted in ICRC commentary that any military objectives located near a combat area would be considered as "part and parcel of the total military system," and further noted that this is the case because it would be

---

[71] *See id.* at 28.
[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] PILLOUD, *supra* note 56, at 673.

https://doi.org/10.59015/wilj.KLCM3237

"difficult to make a clear distinction between military deployment designed to defend the works and installations and other troops fighting in the area."[81] Such an idea translates well to commingled facilities in cyber language: the combat area could be considered the cyberinfrastructure network. Therefore, this Article might indicate that commingled facilities with a connected network might be under the same "military system" and would be indistinguishable to opposing militaries that deploy cyberweapons.

In essence, Article 56 underscores the importance of protecting specific, critical civilian infrastructure, acknowledging its potential to cause significant harm if targeted during armed conflicts.[82] By establishing rules around direct attacks on works and installations containing dangerous forces, this Article aims to strike a balance between military necessity and the protection of essential civilian assets to minimize the effect of hostilities on non-combatants.[83] Here, there are clear protections for nuclear facilities, which is very important for the subject of this Article, especially where facilities have clear commingled networks with military objectives.

d. Article 57

Article 57 of Additional Protocol I to the Geneva Conventions addresses the principle of precautions in attack during armed conflicts.[84] It outlines parties' obligations to take certain precautions to minimize harm to civilians and civilian objects when planning and exercising military operations.[85] Its goal is to strike a balance between military necessity and the protection of non-combatants and their property.[86]

Article 57(1) lays out the overall basis for Article 57.[87] It affirms that during military operations "constant care shall be taken to spare the civilian population, civilians, and civilian objects."[88]

Article 57(2) emphasizes that parties to a conflict must take all feasible precautions in the planning and execution of military operations

---

[81] *Id.* at 674.
[82] *See* Additional Protocol I, *supra* note 27.
[83] *See id.*
[84] *See id.* at 29.
[85] *Id.*
[86] *Id.*
[87] *Id.*
[88] *Id.*

https://doi.org/10.59015/wilj.KLCM3237

to avoid and minimize incidental harm to civilians and civilian objects.[89] Such precautions include verifying that objectives being attacked are not civilian and do not have other special protections; choosing a mean or method of attacking that would avoid, or minimize, loss or injury of civilians or civilian objects; and avoiding launching an attack that may cause excessive "incidental loss of civilian life, injury of civilians, damage to civilian objects, or combination of these" that relates to the military advantage anticipated.[90]

Article 57(3) establishes the solution to the problem of choosing between multiple possible paths.[91] It states that when there is a choice between several different military objectives that would achieve the same or a similar military advantage, a party should select the military objective where the attack is expected "to cause the least danger to civilian lives and to civilian objects."[92]

In summary, Article 57 of Additional Protocol I establishes the obligations for parties to armed conflicts to exercise precaution in attack, aiming to protect civilians and civilian objects.[93] It reflects the humanitarian imperative within the law of armed conflict to mitigate the effect of hostilities on non-combatants and their surroundings.[94] This particular Article, though, only establishes obligations for attacking states to take precautions in order to not harm civilian population.[95] Because this Article's obligates states to choose a means of attack that would do the least harm to civilians, cyberoperations on a commingled facility might be the choice for most states.

e. Article 58

In general, Article 58 of Additional Protocol I to the Geneva Conventions focuses on a state's obligations to protect its own civilians from the effects of attacks.[96] This Article recognizes the importance of those in control of civilian populations to protect their civilians.[97] In other

---

[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] *See generally id.*
[94] *Id.*
[95] *See id.*
[96] *See generally id.*
[97] *See id.*

https://doi.org/10.59015/wilj.KLCM3237

words, this Article, along with Article 57, obligates all parties to a conflict to protect civilians and civilian objects.

This Article has only one paragraph that lays out the obligations states shall uphold when in a conflict, at least to the "maximum extent feasible."[98] First, it obligates states to endeavor to remove any civilian populations and civilian objects within that state's control from the areas where military objectives are taking place.[99] Next, it forbids states from placing military objectives within or near a densely populated area.[100] Last, it outlines general obligations for states to take additional precautions to protect civilian populations and objects under their control from the dangers that may result from military operations.[101]

Article 58 is important, and much commentary has been published on it. First, the ICRC has commented on sub-paragraph (a) stating that moveable civilian objects "should be removed whenever possible away from military objectives." On the other hand, ICRC's comment on immovable objects states that these are "therefore endangered as a result of being in the vicinity of military objectives."[102] As mentioned above, such vicinity in cyber-terms might be connected networks and that vicinity is important when it is proximate to a nuclear facility.

Another important commentary that pertains directly to cyber operations is the Tallinn Manual 2.0.[103] Rule 121 of the Manual suggests that states are obligated to take precautions to protect civilians and civilian objects from the dangers resulting from cyberattacks.[104] The commentary on this rule contemplated a situation where a cyberattack would affect civilian cyber objects, and, in order to prevent that, precautions might include "separating, compartmentalizing, or otherwise shielding civilian cyber systems."[105] (Specific suggestions for this situation will play an important role in the final part of this Article below.) The commentary later indicated that Rule 121 addresses the issue of proximity, whether that is real or virtual, of civilian objects to cyberinfrastructure that "qualifies

---

[98] *Id.*

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] PILLOUD, *supra* note 56, at 694.

[103] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 487 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0].

[104] *Id.*

[105] *Id.* at 490.

https://doi.org/10.59015/wilj.KLCM3237

as a military objective, including dual-use targets."[106] This cements the proximity issue as stated above, mainly that proximity could mean shared networks, and it also indicates that when there is proximity, precautions need to be in place.

In summary, Article 58 of Additional Protocol I shows how important it is for states to take precautions to minimize harm to their civilians and civilian objects.[107] This Article is very important to this Article, and below, this Article will discuss the potential obligations of states to take further precautions to protect civilian populations from a cyberattack on a facility that contains nuclear and cyberweapon development facilities mingled together.

B. SUMMARY OF APPLICABLE ARTICLES

Altogether, the most important articles of Additional Protocol I of the Geneva Conventions to this Article are Articles 51, 52, 56, 57, and 58. Article 51 provides specific protections that are given to civilians during hostilities.[108] This is important because this Article includes an obligation that states not use civilians to shield military objects from attack. Article 52 provides general protection of civilian objects.[109] This helps define the differences between a civilian object and a military objective. Article 56 safeguards installations that contain dangerous forces.[110] This Article is important because it defines when nuclear facilities are protected during conflict. Article 57 obligates attacking states to take constant care to spare civilian populations and civilian objects.[111] This Article lays out the obligations of attacking states and might indicate that cyberattacks are the most likely kind of attack on commingled facilities. Article 58 sets forth precautions that states need to take to protect its own civilian populations and civilian objects from the effects of attacks.[112] This is the most important Article for the thesis of this Article because it sets forth possible obligations of states to protect its own civilian populations and civilian objects under their control and, as discussed below, provide extra

---

[106] *Id.* at 491.
[107] Additional Protocol I, *supra* note 27, at 29.
[108] *See id.* at 26.
[109] *See id.* at 27.
[110] *See id.* at 28.
[111] *See id.* at 29.
[112] *See id.*

https://doi.org/10.59015/wilj.KLCM3237

precautions from attacks when nuclear and cyberweapon development facilities are commingled.

II. COMBINING NUCLEAR AND CYBER CAPABILITIES

Nestled in the Snake River plains of southeast Idaho lies the small rural town of Idaho Falls. About an hour's drive west of Idaho Falls is the Idaho National Laboratory's (INL) nuclear reactor facility. It is located not too far from Arco, ID, the first city to be powered entirely by nuclear power in the United States.[113] For those who grew up in Idaho Falls, their parents typically worked doing one of four things: working in the medical field, being an attorney, working for a local company health company, or, the most popular option, working out at the INL. The Laboratory is not only known locally, but it is also well known nationally for its development of new nuclear technology that moves the sustainable energy field forward. The INL's website emphasizes that the INL's mission "is to discover, demonstrate and secure innovative nuclear energy solutions, other clean energy options and critical infrastructure."[114]

However, another branch of the INL that most people do not know about (both locally and nationally) is the INL's Cyber National Security Department. Most do not realize that the INL has a large division tasked with creating effective cyber malware products. In fact, some believe that the INL had a hand in the cyberweapon, Stuxnet, used on the nuclear facility in Natanz, Iran. As alluded to earlier, Israel likely got help from a much larger Western ally in the operation leading up to the deployment of the malware.[115] There is considerable speculation that researchers at the INL may have been responsible for passing on critical information relating to the Stuxnet malware before it was released in Iran.[116]

It, therefore, appears that the United States of America is engaging in the type of activity at the INL that this Article is focused on. At the INL, the United States has commingled nuclear and cyberweapon development facilities into a single cyberinfrastructure system. For that reason, it is

---

[113] *FAQ*, CITY OF ARCO IDAHO, https://cityofarco.municipalimpact.com/faq [https://perma.cc/JF75-KQG8] (last visited Mar. 15, 2024).

[114] *Vision, Mission and Leadership*, IDAHO NAT'L LAB'Y, https://inl.gov/about-inl/organization/ [https://perma.cc/27TE-6UDS] (last visited Mar. 15, 2024).

[115] Gross, *supra* note 2.

[116] Kim Zetter, *Did a U.S. Government Lab Help Israel Develop Stuxnet*, WIRED (Jan. 17, 2011, 10:13 PM), https://www.wired.com/2011/01/inl-and-stuxnet/ [https://perma.cc/U2SX-EDUS].

https://doi.org/10.59015/wilj.KLCM3237

essential for the United States to understand the international law implications for this commingling under the law of armed conflict.

Of course, it is important to note here that this Article is not meant to just apply to the United States; the principles here would apply to any state that decides to engage in such commingling as discussed herein, especially in times of international war when the laws of armed conflict and Additional Protocol I would apply.

A. LOSS OF PROTECTIONS FOR NUCLEAR FACILITIES

Just over a three-hour southeast drive from Baghdad, Iraq, resides the famous temple of Ur-Nammu.[117] The temple is located in the city of Ur, which, famously, is the birthplace of the biblical patriarch Abraham.[118] The temple, or ziggurat, is quite possibly the most spectacular archeological site in all of Mesopotamia, with most of the original pyramid-shaped structure still standing today.[119] During the Gulf War of 1990, it was reported that Iraqi President Saddam Hussein placed two Soviet-made MIG-21 fighter bombers next to the temple, hoping to shield the MIGs from being targeted by opposing forces.[120] The conventional thinking at the time was that because Article 53 of Additional Protocol I, as well as the 1954 Hague Conventions, stated that cultural property was not to be destroyed from the foreseeable effect of armed conflict, the MIGs placed near them could not be targeted.[121] This was the case because an attack on the MIGs would destroy the cultural temple of Ur-Nammu as well.[122] Dick Cheney, the US Defense Secretary at the time, argued that Hussein's decision to put the planes next to the temple made Iraq responsible for any unintended destruction caused by bombers.[123] This should be the case, Cheney claimed, because the placement at the site was

---

[117] Oswald Johnston, *Iraqis Put Warplanes at Ancient Temple, U.S. Says: Archeology Secretary Cheney Says MIGs Are Next to Ruins of Historic Site. Hussein Reportedly Has Customarily Placed Military Installations Near Cultural Locations*, LA TIMES (Feb. 14, 1991, 12:00 AM), https://www.latimes.com/archives/la-xpm-1991-02-14-mn-1799-story.html [https://perma.cc/PRV6-WHZ4].

[118] *Id.*

[119] *Id.*

[120] *Id.*

[121] Additional Protocol I, *supra* note 27, at 26; *Convention for the Protection of Cultural Property in the Event of Armed Conflict with Regulations for the Execution of the Convention*, UNESCO, https://en.unesco.org/sites/default/files/1954_Convention_EN_2020.pdf [https://perma.cc/BZR5-U6CW] (last visited Mar. 28, 2024).

[122] Johnston, *supra* note 117.

[123] *Id.*

https://doi.org/10.59015/wilj.KLCM3237

"obviously an effort to use the archeologically significant facility to protect his military capabilities."[124] Later, however, when coalition leaders stated in a public forum that they would not target religious sites, "Saddam began using these sites to shield military equipment and units" even more.[125]

The question that arises here is parallel with the question of combining nuclear and cyberweapons development facilities: whether the military objectives connected to this culturally protected place can be targeted by an opposing state. Though states might decide not to destroy the protected sites, like the United States in 1991,[126] such sites would be targetable under two theories. First, the civilian objects, because of their use or location and purpose under Article 52(2) of Additional Protocol I, have become military objectives and therefore can be targeted.[127] And, second, the civilian objects lose their protections under Article 51(7) of Additional Protocol I because the state is using the civilian objects "in order to attempt to shield military objectives from attacks or to shield military operations."[128]

Next, this Article will detail how these two theories allow targeting of the commingling of protected objects and why specifically combining a nuclear facility and cyberweapon development would make the nuclear facility a target for a cyberattack. Following that, this Article will discuss the responsibilities of both the attacking state and the state that combined such facilities to mitigate the potential fallout of an attack.

1. Theory One: Article 52

As discussed above, Article 52 of Additional Protocol I outlines the general protections for civilian objects.[129] It states that "civilian objects shall not be the object of attack."[130] On the other hand, it also states that "attacks shall be limited only to military objectives."[131] According to this

---

[124] *Id.*

[125] *Crafting Tragedy*, THE WHITE HOUSE: PRESIDENT GEORGE W. BUSH, https://georgewbush-whitehouse.archives.gov/ogc/apparatus/crafting.html [https://perma.cc/ZK4W-XCL2] (last visited Mar. 28, 2024).

[126] *Id.*

[127] Additional Protocol I, *supra* note 27, at 27.

[128] *Id.* at 26.

[129] *Id.* at 27.

[130] *Id.*

[131] *Id.*

https://doi.org/10.59015/wilj.KLCM3237

Article, there are two requirements in order for something to become a military objective.[132] First, the "nature, location, purpose or use" must contribute to a "military action."[133] Second, the destruction must offer a "military advantage."[134] The question then becomes whether a nuclear facility is converted to a military objective because of its connection to a cyberweapon development facility, according to Article 52.

First, under the first prong, there are two theories that would satisfy it: first, the dual-use theory, and second, the location and purpose theory. According to the dual-use theory, the question is, does a nuclear facility commingled with cyber weapons development become a military objective because of its nature, location, purpose, or use? The question here relies on whether the cyber weapons development facility has become so connected to the nuclear facility that it becomes dual-use and, therefore, a military objective.[135] Dual-use infrastructure (used both for civilian and military benefit) is considered a military objective and can be targeted.[136] In this case, the dual-use nature is that the nuclear facilities are used by civilians while the cyber weapons facilities are used for military purposes. The question then comes down to whether the commingling of such facilities is to a point where it is not possible to distinguish between the two.[137] In the case where a cyberattack is contemplated, this determination is based on the connection of computer infrastructure. This would have to be done on a case-by-case basis to determine the extent to which the objects are separated and thus separately targetable.[138] However, in the case where the facilities are so mingled that they are indistinguishable,[139] they would be dual-use, and, because the cyberweapons development side is, by its "use," military, the whole system, including the nuclear facility, is a military objective and targetable.

As mentioned above, the ICRC, in their Article 56 commentary, contemplated the implications of a military objective located near nuclear facilities.[140] They indicated that when this happens, the entire object

---

[132] PILLOUD, *supra* note 56, at 635.

[133] *Id.*

[134] *Id.*

[135] *See* Laurie R. Blank, *Extending Positive Identification from Persons to Places: Terrorism, Armed Conflict, and the Identification of Military Objectives*, 2013 UTAH L. REV. 1227, 1252 (2013).

[136] *Id.*

[137] *See id.*

[138] *Id.*

[139] *See generally id.*

[140] PILLOUD, *supra* note 56, at 674.

https://doi.org/10.59015/wilj.KLCM3237

becomes part of the "total military system."[141] Here, in the case of cyberinfrastructure, geographical location is less important. Instead, network sharing would indicate proximity and make geographically separate nuclear and cyber facilities part of the same military dual-use system because their networks are shared.[142]

Alternately, there is another argument that would not require the facilities to be so mingled that they have become one and, therefore, dual use. This theory is called the location and purpose theory. Because of the proximity of the nuclear facility to the cyberweapons development facility, its location and purpose make the nuclear facility a military objective.[143] This is because the proximity of the nuclear facility can be considered an attempt to shield the cyberweapons facility from attacks. Therefore, because of the nuclear facility's network cyberlocation in relation to the cyberweapon facility—a military objective by use and nature—and because the nuclear facility's purpose is to protect the cyber facility, the nuclear facility is a military objective and could be the object of an attack where an attack will not "cause the release of dangerous forces and consequent severe losses among the civilian population" as found in Article 56 of Additional Protocol I.[144]

With that being said, under the dual-use theory and the location and purpose theory, the nuclear facility would be contributing to a military action. Military action means that the object is recognized as being of military interest.[145] In the case that the commingling leads to the objects being seen as dual use, the use of both the nuclear and cyber facilities contribute to a military action because weapons, whether they are tangible or cyber, are recognized as being of military interest, satisfying this prong of the analysis.[146] If the location or purpose leads the analysis, the nuclear facility contributes to a military action because the facility is being used as a cover for the cyberweapons development, which is an interest of an opposing military. Therefore, in both cases, the dual use of the nuclear facility, or its purpose and location, contributes to a military action.

Second, Article 52 requires that the destruction of an object must create a military advantage.[147] This is designed to prohibit attacks that only

---

[141] *Id.*

[142] *See* TALLINN MANUAL 2.0, *supra* note 103, at 490-91.

[143] PILLOUD, *supra* note 56, at 636.

[144] Additional Protocol I, *supra* note 27, at 28.

[145] PILLOUD, *supra* note 56, at 638.

[146] *Id.* at 635.

[147] *Id.* at 636.

https://doi.org/10.59015/wilj.KLCM3237

offer potential or indeterminate advantages.[148] Therefore, military advantages should be concrete and direct.[149] Under the first prongs dual-use theory, it can easily be seen how an attack on the facility would lead to a military advantage. This is because an attack would destroy the cyberweapons capabilities of such a facility. Any destruction of the dual-use facility would then be justified, even including the nuclear portion of the facility, if that occurred. On the other hand, it is not clear, under the purpose or location theory, that an attack on the nuclear facility rather than the cyber facility provides a military advantage. This is because while destroying the cyber facility would offer a military advantage, but specifically targeting and destroying the nuclear facility would not provide the same advantage because the cyber facility would still be operational. Further, destroying the shield, but not the military objective being shielded, does not provide a military advantage. Therefore, under this particular theory, the nuclear facility would not be seen as a military objective and could not be targeted alone.

With that being said, if the facility is seen as dual use, targeting the facility would be allowed as long as the attack complied with Article 56 of Additional Protocol I in that such an attack would not cause severe losses among the civilian population. On the other hand, if the nuclear facility falls within the location or purpose justification, the nuclear facility cannot solely be targeted because it would not provide a military advantage to destroy alone. Next, this Article will discuss the second theory of how a state may lose protections for a nuclear facility when it commingles such a facility with a cyberweapons development facility.

2. Theory Two: Article 51

The second theory for why commingling nuclear facilities with cyber facilities would cause a state to lose protections for the nuclear facilities is recited in Article 51 of Additional Protocol I and is analogous to the prohibition on human shields.[150] Article 51(7) states that the presence of civilians cannot be used to "render certain points or areas immune from military operations."[151] In particular, this Article prohibits

---

[148] *Id.*

[149] *Id.* at 637.

[150] Additional Protocol I, *supra* note 27, at 26.

[151] *Id.*

https://doi.org/10.59015/wilj.KLCM3237

states from shielding military objectives from attacks.[152] Of course, this provision, in particular, was written to prohibit the use of human shields, but this prohibition can also be used to prohibit other types of shields.[153] In particular, the United States claimed this Article was a legal justification for a potential attack on the military aircraft—if they chose to—placed next to the temple of Ur-Nammu.[154] The United States claimed that because Hussein was trying to shield military objectives by placing them next to civilian objects and cultural heritage sites, they could still target the military objectives and that the temple site lost its legal protection because of the shielding.[155]

Such an analysis would apply to this Article's thesis as well. A reason to commingle cyber operations with nuclear facilities is to shield the cyber facilities from a cyberattack by including them with the protected nuclear facilities. However, this does not prohibit states from committing a cyberattack on the cyber facility, and any collateral damage to the nuclear facility would be acceptable. A state using this type of shielding method is trying to use the nuclear facility's protections to its advantage to shield the cyberweapon development facility from attacks. Therefore, a state may still be able to target the cyber operations and any collateral damage to the nuclear facility would be acceptable.

As mentioned above, the ICRC, in its Article 51 commentary, tied the provision on human shields in Article 51 to Article 12(4) of Additional Protocol I.[156] It compared using human shields to using other objects, like medical units, as shields and stated that these other shields should additionally be prohibited according to this Article.[157] From that line of thinking, other protected objects could be included in this prohibition, such as objects containing dangerous forces like nuclear facilities. Therefore, using a nuclear facility as a shield could also be prohibited under this Article.

Under either Article 51 or Article 52 of Additional Protocol I, when a state commingles its nuclear facilities with cyberweapons development, it cannot shield the cyberweapons from attack because of the proximity to the nuclear facilities. The cyber facility can be targeted despite the potential collateral damage to the nuclear facilities. Next, this

---

[152] PILLOUD, *supra* note 56, at 627.
[153] *See generally Crafting Tragedy*, *supra* note 125.
[154] Johnston, *supra* note 117.
[155] *See generally Crafting Tragedy*, *supra* note 125; Johnston, *supra* note 117.
[156] PILLOUD, *supra* note 56, at 627.
[157] *Id.*

https://doi.org/10.59015/wilj.KLCM3237

Article will briefly discuss the obligations of the attacking state when it targets commingled facilities. Then, this Article will discuss the obligations of states that combine such facilities to take precautions to protect their commingled facilities from cyberattacks.

III. OBLIGATIONS OF THE ATTACKING STATE

The obligations of a state attacking a nuclear facility are outlined in Articles 57 and 56 of Additional Protocol I.[158] From Article 57, two main provisions apply to this situation.[159] First, those who plan an attack should take all feasible precautions in the choice of means and methods of the attack to avoid injury or death to civilians.[160] Next, when there is a choice between several military objectives that obtain a similar military advantage, the one that causes the least amount of danger to civilians should be selected.[161]

The first obligation comes from Article 57, sub-paragraph (a)(ii).[162] In cases where an attack on a certain facility is necessary to gain a military advantage, states must do so in a way that causes the least amount of civilian harm.[163] It is important to note that commingling nuclear and cyber facilities would not only allow states to target the facility through cyberwarfare, but would also allow more direct means, such as through kinetic attacks.[164] However, because of the nuclear nature of these facilities, attacking states must account for the potential harm attacking the facility would have on civilian populations. Because of this, if the state has the capabilities, the best means (that would cause the least amount of harm to civilians) is cyberwarfare under this Article.

The second obligation falls within paragraph 3 of Article 57.[165] According to this provision, if a state has a choice between attacking several military objectives, especially where a similar outcome could be achieved at each, the state should choose the objective that would cause

---

[158] Additional Protocol I, *supra* note 27, at 28-29.

[159] *See id.* at 29.

[160] *Id.*

[161] *Id.*

[162] *Id.*

[163] PILLOUD, *supra* note 56, at 682-83.

[164] *See generally* Carlos Plazas, *Information Crossroads: Intersection of Military and Civilian Interpretations of Cyber Attack and Defense*, 5 U. CINCINNATI INTELL. PROP. & COMPUT. L.J. (2021).

[165] Additional Protocol I, *supra* note 27, at 29.

https://doi.org/10.59015/wilj.KLCM3237

the least amount of harm to civilians.[166] This is a provision that states must remember when attacking a commingled facility by cyber means. However, it is unlikely that the state could achieve the military advantage it seeks without attacking the cyberweapons development facility. So, even though a state should keep this in mind, the provision likely will not stop a state from choosing to attack a commingled facility.

Last, according to Article 56 of Additional Protocol I, an attacking state needs to consider the possible effects when damage is done to nuclear facilities.[167] Paragraph 3 of this Article states that when a nuclear facility is attacked, "all practical precautions shall be taken to avoid the release of the dangerous forces."[168] This call for protection is made in order to protect against the harm that could be done to civilians near such a facility.[169] This, again, is something that should be considered when a state is planning to attack commingled facilities. Still, this provision may not stop the state from following through with the attack, especially when the attack is executed through cyber means.

The underlying reason for all three of the provisions mentioned, is to protect civilian populations.[170] When states attack commingled facilities, they should try to reduce the harm to civilian populations. Some states might choose to do this by attacking such facilities through cyber means. Doing this would likely fulfill the obligations of attacking states that arise under the above Articles. Next, this Article will discuss the particular obligations that states inherit when they combine nuclear and cyber warfare weapon development facilities.

IV. OBLIGATIONS OF THE COMMINGLING STATE

During the Lebanon War in 2006, it was reported that Hezbollah would often use Lebanese civilians as human shields in order to dissuade the IDF from firing at their gunman and rocket launchers.[171] Even the Human Rights Watch concluded that "Hezbollah occasionally did store

---

[166] *Id.*

[167] *Id.* at 28.

[168] *Id.*

[169] *See id.*

[170] *See generally id.* at 28-29.

[171] SPME, *Annan's Claims on Casualties May Unravel by Benny Avni – Staff Reporter of the Sun, 7.27.06*, SCHOLARS FOR PEACE IN THE MIDDLE E. (July 28, 2006), https://spme.org/news-from-the-middle-east/annans-claims-on-casualties-may-unravel-by-benny-avni-staff-reporter-of-the-sun-7-27-06/1503/ [https://perma.cc/2Y9B-D9A5].

https://doi.org/10.59015/wilj.KLCM3237

weapons in or near civilian homes and fighters placed rocket launchers within populated areas or near U.N. observers."[172] On July 25, 2006, Israeli forces attacked and destroyed a U.N. observer post in southern Lebanon in an attack on Hezbollah, leading to multiple casualties.[173] One of those killed in the attack was Canadian Major Paeta Derek Hess-von Kruedener.[174] Just before the attack, the Canadian Major sent an email to Major-General Lewis MacKenzie.[175] In the email, he stated, referring to Israeli action, "the closest artillery has landed within two meters of our position, and the closest 1,000 lbs. aerial bomb has landed 100 meters from our patrol base. This has not been a deliberate targeting, but rather due to tactical necessity."[176] Major-General MacKenzie later interpreted it for a reporter, stating, "what that means, in plain English, 'We've got Hezbollah fighters running around in our positions, taking our positions here and then using us for shields and then engaging the (Israeli Defense Forces).'"[177]

In cases of blatant military tactics to shield operations using civilians and civilian objects, who should be held responsible for the casualties that occur? In the case above, even the Canadian Major agreed that the attacks were a military and tactical necessity for the IDF in order to fight the Hezbollah forces.[178] Is Israel the only culpable party, or does the party employing the shield hold any responsibility for the casualties that are a direct result of the use of the shield? According to Article 58 of Additional Protocol I, states must take "necessary precautions to protect the civilian populations, individual civilians and civilian objects."[179]

The next part of this Article will discuss the obligations of states that have control over commingled nuclear and cyber facilities. First, this Article will discuss the underlying legal theory for applying obligations. Then, the Article will discuss the precautions that states must take for cyberattacks when they commingle nuclear and cyber facilities.

---

[172] *Fatal Strikes*, HUM. RTS. WATCH (Aug. 2, 2006), https://www.hrw.org/report/2006/08/02/fatal-strikes/israels-indiscriminate-attacks-against-civilians-lebanon [https://perma.cc/4T59-Z6KQ].

[173] *Israeli Bomb Kills UN Observers*, BBC (July 26, 2006), http://news.bbc.co.uk/2/hi/5215366.stm [https://perma.cc/LTH7-Z94J].

[174] Joel Kom, *Hezbollah Was Using UN Post as 'Shield*,*'* OTTAWA CITIZEN (July 27, 2006), https://web.archive.org/web/20070517040057/http://www.canada.com/ottawacitizen/news/story.html?id=37278180-a261-421d-84a9-7f94d5fc6d50 [https://perma.cc/JE7C-3DGV].

[175] *Id.*

[176] *Id.*

[177] *Id.*

[178] *Id.*

[179] Additional Protocol I, *supra* note 27, at 29.

https://doi.org/10.59015/wilj.KLCM3237

A. INTERNATIONAL LEGAL BASIS

The above-mentioned Human Rights Watch report created during the 2006 Lebanese War stated that the placement of weapons near civilian homes and rocket launchers placed near UN observers was a "serious violation of the laws of war because they violate the duty to take all feasible precautions to avoid civilian casualties."[180] For this reason, there seems to be an international understanding of some sort of obligation imposed on states that use human shields.[181] But under what international laws are obligations created? Next, this Article will discuss two possibilities: first, an analogy to the United States and other countries' policies on human shields, and second, from Additional Protocol I, Article 58.

1. US Policy on Human Shields

The United States' views on the use of human shields are similar to many other countries on the matter. For example, during the 2006 Lebanon War, the Israeli forces felt justified in their continued attack on Hezbollah forces even though Hezbollah forces were actively using human shields.[182] Their view was that Hezbollah was responsible for the deaths of civilians when determining the proportionality of an attack.[183] These same views can be found in the United States Department of Defense Law of War Manual.[184]

Section 5.12.3.4 of the Department of Defense Law of War Manual states that the "use of . . . human shields violates the rule that protected persons may not be used to shield . . . military operations. The party that employs human shields in an attempt to shield military objectives from attack assumes responsibility for their injury."[185] Although not the position of all states, the US has shown that when an attack harms civilians because a human shield was used, the state using these shields is responsible for the harm caused.

---

[180] *Fatal Strikes*, *supra* note 172.
[181] *See generally id.*
[182] SPME, *supra* note 171.
[183] *See generally id.*
[184] *See generally* OFF. OF GEN. COUNS. DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL § 5.12.3.4 (2023).
[185] *Id.*

https://doi.org/10.59015/wilj.KLCM3237

This type of analysis should also be applied when states use civilian objects to try to shield military objectives. In particular, using a nuclear facility to shield a cyberweapons development facilities from cyberattacks would make the state deploying this tactic responsible for any damage to the nuclear facility during an attack. Therefore, it is the state's responsibility to protect civilian objects that contain dangerous forces from cyberattacks, and the state would be responsible for any harm to civilians if it does not protect such installations from an attack.

Therefore, by analogizing to the US's position, states that deploy a tactic in which they use a nuclear facility to shield a cyberweapons development facility from cyberattacks, the shielding state would bear the responsibility for harm caused to the nuclear facility as a result of an attack. Therefore, the state has some responsibility to enact safeguards in order to protect civilian populations from any possible dangerous forces that the nuclear facility could release. Next, this Article will discuss the obligations that arise under Article 58 of Additional Protocol I to take precautions against the effects of attacks.

2. Article 58 Additional Protocol I: Precautions Against the Effects of an Attack

As discussed above, Article 58 of Additional Protocol I deals with the obligations of states to protect their own civilian populations and objects from the effects of attacks.[186] The Article starts by saying that a party to a "conflict shall, to the maximum extent feasible," meet three conditions.[187] First, civilian populations and objects under the state's control should be removed from the location of military objectives.[188] Next, military objectives should not be located near densely populated areas.[189] Last, states must take necessary precautions to protect civilian populations and objects under their control against the dangers resulting from military operations.[190]

In Article 58 under subparagraph (a), civilian objects that are more permanent and cannot be removed are endangered due to being in the vicinity of military objectives.[191] Therefore, there is an obligation to

[186] Additional Protocol I, *supra* note 27, at 29.
[187] *Id.*
[188] *Id.*
[189] *Id.*
[190] *Id.*
[191] *Id.*

https://doi.org/10.59015/wilj.KLCM3237

separate military objectives from civilian objects where feasible. This paragraph seems to imply that states should not commingle civilian and military facilities. However, where states do choose to commingle, the state is responsible for the damage that might be done to civilian objects as a result of an attack. In the particular case of nuclear and cyber facilities, the proximity might not necessarily be geographical but rather via network. If the same governing organization covers both facilities and their networks are mingled, a cyberattack on the cyber branch could leak over to the nuclear and civilian branches and cause computer damage to those systems. This paragraph of Article 58 seems to obligate states to segregate such networks. If that is not feasible, the state has endangered the nuclear civilian branch, which might cause civilian harm.[192] In such a case, it is a breach of this Article, and the controlling state might be liable for the effects rather than the attacking state.

The last paragraph of Article 58, paragraph (c), obligates states to take other necessary precautions.[193] It seems the drafters of this Article were less worried about listing out all the precautions they felt states would need to take and more inclined to create a legal obligation that could change based on the state's civilian population's needs. For that reason, this paragraph was likely included to protect civilians and civilian objects from military operations on more of a case-by-case basis. In particular, the ICRC commentary to this Article states that civilian objects "are entitled to special protection should be kept in mind, such as . . . works containing dangerous forces."[194] Therefore, in the case of commingled nuclear and cyber facilities, this Article provides an obligation to enact necessary precautions against cyberattacks on such a facility. Potentially obligated precautions against a cyberattack will be discussed further below.

Under Article 58 of Additional Protocol I, paragraphs (a) and (c), states have a duty to remove civilian objects from the vicinity of military objects as well as to take necessary precautions to protect civilian objects.[195] In the case where nuclear and cyber facilities are commingled, the state has a duty to try to separate those facilities; if it does not, or it is not feasible, the state is still obligated to take other necessary precautions to protect the nuclear branch from cyberattacks. These responsibilities may arise out of a similar analysis as US policy, but such responsibilities

---

[192] TALLINN MANUAL 2.0, *supra* note 103, at 490-91.
[193] Additional Protocol I, *supra* note 27, at 29.
[194] PILLOUD, *supra* note 56, at 695.
[195] Additional Protocol I, *supra* note 27, at 29.

https://doi.org/10.59015/wilj.KLCM3237

and obligations also arise under Article 58 of Additional Protocol I. Next, this Article will discuss some of the potential safeguards that states can employ that would adequately fulfill their obligations to protect nuclear facilities from cyberattacks on a commingled facility.

V. PRECAUTIONS REQUIRED

On November 19, 2023, the Idaho National Laboratory (INL) suffered a significant data breach that leaked a treasure trove of information.[196] The information included "employee addresses, Social Security numbers, bank account information, full names, employee information, and dates of birth."[197] After the incident, the INL quickly coordinated with the FBI and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency in order to investigate and understand the "scope and impact of the breach."[198] Colin Little, a security engineer at Centripetal, commented on the incident, stating, "although media surrounding this event claims that no nuclear secrets . . . was accessed or stolen, which is fortunate, it is nonetheless highly disconcerting that the staff generating that . . . and participating in the most advanced Nuclear Energy R&D have had their information leaked online."[199] Interestingly enough, the perpetrators of this particular attack were not state-sponsored but were a known pro-Russian hacktivist group.[200] An incident like this is concerning. Even though it was not a cyberattack as defined by the law of armed conflict, it provides an example of the vulnerabilities of the cyber security infrastructure of a location that has commingled nuclear and cyber weapon facilities.

First, it is important to note that there is much that the United States and the INL do to protect themselves from cyberattacks. After the advent of what we know as the World Wide Web, by the late 1990s, the world's use of the internet was widespread. The United States federal government and other national governments quickly took many steps to

---

[196] Kristina Beek, *Idaho National Nuclear Lab Targeted in Major Data Breach*, DARK READING (Nov. 22, 2023), https://www.darkreading.com/ics-ot-security/idaho-national-nuclear-lab-targeted-in-major-data-breach [https://perma.cc/5LTY-537R].

[197] *Id.*

[198] *Id.*

[199] *Id.*

[200] Alicia Hope, *Furry Hacktivists Breached Nuclear Lab and Stole Employee Data*, CPO MAG. (Nov. 30, 2023), https://www.cpomagazine.com/cyber-security/furry-hacktivists-breached-nuclear-lab-and-stole-employee-data/ [https://perma.cc/2MHR-EV8A].

https://doi.org/10.59015/wilj.KLCM3237

provide general protection over the course of the next decades.[201] It is not essential to list all these cybersecurity-related protections here. Instead, this Article focuses on further precautions states can take to protect nuclear facilities that are commingled with cyber weapons facilities from the harm of cyberattacks. Nonetheless, the recommendations here might be some that the United States and other countries with commingled nuclear and cyber weapons facilities have already employed. This Article aims to highlight the obligations and what states need to do according to those obligations derived from Article 58 of Additional Protocol I.

The question then is what specific systems or precautions should be taken in order to protect these commingled nuclear cyber facilities from cyberattacks. This Article suggests seven separate and specific solutions that states that have commingled facilities can implement in order to fulfill their obligations under Article 58 of Additional Protocol I to take precautions against the effects of an attack.[202] A state should take the following precautions: segregate networks, set up firewalls and intrusion detection systems, set up access control and authentication, input patch management, hold security monitoring and logging, implement vendor risk management, and maintain continuous improvements. These seven recommendations will help co-mingled facilities and the states that govern them to be compliant with their Article 58 obligations.

A. NETWORK SEGMENTATION

First, commingled facilities should implement systems where they can segment the networks of the nuclear branch and cyber branch within the facilities' control. Network segmentation is a network security technique that divides a more extensive network into smaller, distinct subnetworks so that network teams can compartmentalize these subnetworks.[203] The result is the ability to "deliver unique security controls and services to each sub-network."[204] Once subdivided networks exist, control should be applied to each individual, compartmentalized

---

[201] *See generally* Michael Brands, *Cybersecurity Regulations and Laws*, CONNECTWISE (May 6, 2024), https://www.connectwise.com/blog/cybersecurity/cybersecurity-laws-and-legislation [https://perma.cc/W38M-AC92].

[202] Additional Protocol I, *supra* note 27, at 29.

[203] *What Is Network Segmentation?*, VMWARE, https://www.vmware.com/topics/network-segmentation [https://perma.cc/BPJ9-WN98] (last visited Apr. 5, 2024).

[204] *Id.*

https://doi.org/10.59015/wilj.KLCM3237

segment.[205] The main reason for segmenting the networks into the nuclear network and the cyber network at these facilities is because a network is only as strong as its weakest link. The reality is that "a large flat network inevitably presents a large attack surface."[206] Working to segment and isolate the networks reduces the attack surface and impedes the potential lateral movement of malware. This would help protect the nuclear facility's network from cyberattacks on the cyberweapons development facility's network. Therefore, segmenting the networks at a commingled facility is an important precaution that a state should take.

B. FIREWALLS AND INTRUSION DETECTION/PREVENTION SYSTEMS

Second, these facilities should implement firewalls and intrusion detection systems in order to detect and block potential cyberattacks that leak their way to the nuclear side of the facility. Generally, there are two types of firewalls: software-based personal firewalls and network-based hardware firewalls.[207] Software-based firewalls are, in essence, extensions of a workstation's operating system, while network-based firewalls are hardware appliances that "physically pass traffic using the same mechanisms as network routers and switchers."[208] Both kinds of firewalls should be implemented because they can protect a nuclear facility from cyberattacks not only on a large-scale network level but also on the smaller, workstation level, protecting a larger scope of the facility.

An intrusion detection system is installed on a server and reviews all of a network's traffic that passes through the server in order to look for and find network traffic that is suspicious in nature.[209] An intrusion prevention system can then block or prevent suspicious traffic from proceeding, effectively ending the network conversation with the potential malware.[210] The difference between intrusion prevention and firewalls is that while firewalls make their decisions on IP addresses, intrusion prevention systems make "decisions based on message content."[211]

---

[205] *Id.*

[206] *Id.*

[207] *Firewalls, Intrusion Prevention and VPNs*, UNIV. OF HOUS. CLEAR LAKE, https://www.uhcl.edu/information-security/tips-best-practices/firewalls [https://perma.cc/8GX9-4QCU] (last visited Apr. 5, 2024).

[208] *Id.*

[209] *Id.*

[210] *Id.*

[211] *Id.*

https://doi.org/10.59015/wilj.KLCM3237

Implementing both kinds of protective systems at multiple levels—at the network, server, and workstation level—would help prevent any leaked cyberattacks meant for the cyber facilities from harming the nuclear facilities system and help a state comply with their precautions obligations under Article 58.

C. ACCESS CONTROL AND AUTHENTICATION

Third, these facilities should make sure to control access and implement authentication systems in order to protect against the leak of cyberattacks from the cyberweapons facility to the nuclear facility. Authentication and authorization are processes that verify the identity of a user trying to access a system, access data, or perform some action.[212] Having this system in place would prevent cyberattack infected computers or devices from being able to connect to and infect the nuclear cybernetwork. This might be a simple means to protect the nuclear facility from cyberattacks, but it is another way to prevent leakage of an attack, helping to fulfill a state's obligation to take precautions.

D. PATCH MANAGEMENT

Fourth, these facilities should make sure that they are effectively managing patches in order to prevent potential vulnerabilities from harming the nuclear facility. Patch management is a phrase used to describe the process of "applying updates to software, drivers, and firmware to protect against vulnerabilities."[213] Patch management should be used on both employee laptops and user-less PC-based devices.[214] Keeping device patches up to date helps protect from cyberattacks and keeps devices running at their highest performance.[215] Keeping systems up to date with the latest technology to protect against leaked cyberattacks is crucial. Technology changes every day and so does the sophistication of cyberweapons. Maintaining effective patch management at nuclear

---

[212] *Authentication Versus Access Control*, IBM (Mar. 4. 2021), https://www.ibm.com/docs/en/wca/3.5.0?topic=security-authentication-versus-access-control [https://perma.cc/DWJ6-PWB7].

[213] *What Is Patch Management?*, INTEL, https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/patch-management.html [https://perma.cc/SQE8-53DG] (last visited Apr. 5, 2024).

[214] *Id.*

[215] *Id.*

https://doi.org/10.59015/wilj.KLCM3237

facilities will help protect nuclear facilities from the harm of leaked cyberattacks on cyber facilities and is a precaution states should take in order to comply with Article 58.

E. SECURITY MONITORING AND LOGGING

Fifth, these facilities should implement security monitoring systems that continue to learn because of the ever-changing cyber warfare landscape. Security information and event management software should act much like a digital immune system, not just fighting off potential harm, but also learning from it.[216] Therefore, systems should use AI properties in order to understand and keep up with an ever-changing problem.[217] These systems will not only be able to stop threats but also identify and eradicate malware, if found.[218] This is all possible because of monitoring and logging, which helps cybersecurity learn and improve over time.[219] Nuclear facilities that are commingled with cyberweapons facilities should implement security monitoring and logging in order to learn and improve over time. Because of the ever-changing field of cyber weapons sophistication, nuclear facilities should implement security monitoring systems that use AI learning as a precaution against the harm of a cyberattack on the cyber facilities.

F. VENDOR RISK MANAGEMENT

Sixth, these facilities should make sure to have a proper system in place to monitor the risks of using vendor services. Specifically, facilities should regularly assess and manage the cybersecurity risks associated with vendors that have access to critical systems.[220] Such management should include ensuring that contractual agreements with vendors include provisions for security controls and incident response capabilities. The main issue here is that the use of third-party vendors should not increase

---

[216] Jason Miller, *What Is Security Logging and Monitoring?*, BITLYFT (May 2, 2019), https://www.bitlyft.com/resources/what-is-security-logging-and-monitoring [https://perma.cc/74KE-4YRK].

[217] *Id.*

[218] *Id.*

[219] *Id.*

[220] Jake Olcott, *What Is Vendor Risk Management (VRM)?*, BITSIGHT (Sept. 26, 2024), https://www.bitsight.com/blog/vendor-risk-management-definition [https://perma.cc/GJH3-4KLT].

https://doi.org/10.59015/wilj.KLCM3237

the possibility of cyberattack leakage harm on the nuclear facilities from an attack on the cyber weapons facilities. States are obligated under Article 58 to make sure that vendors do not increase the risk of harm from cyberattacks.

G. CONTINUOUS IMPROVEMENT

Seventh, these facilities should continually make improvements to cybersecurity, producers, and technologies in order to stay up to date across the board. Regular reviews and updates, including audits, can be useful to identify areas of cyberinfrastructure that need improvement. Again, because of the ever-changing advancements in cyberweapons, nuclear facilities must keep up with advancements in cyber-defense. Therefore, states should take precautions to continue improving cyber-defense systems at nuclear facilities that are commingled with cyber facilities in order to protect them from harm from a cyberattack on the cyber facility.

A state must take precautions to protect nuclear facilities from leakage from a cyberattack. It can do this by implementing these seven recommendations: segregate networks, set up firewalls and intrusion detection systems, set up access control and authentication, input patch management, hold security monitoring and logging, implement vendor risk management, and maintain continuous improvements. These seven recommendations will help states that govern commingled facilities comply with their Article 58 obligations to take precautions against the effects of cyberattacks.

VI. CONCLUSION

States in a time of war have a duty under the law of armed conflict not to attack installations containing dangerous forces, such as nuclear-generating stations, because of the harm they can cause to civilians.[221] However, when states commingle nuclear development facilities and the development of malicious cyberwarfare weapons within the same cyberinfrastructure, they forfeit protections under the law of armed conflict that would prohibit states from attacking said nuclear facilities.[222] States that combine these industries inherit a significant duty to take

[221] Additional Protocol I, *supra* note 27, at 28.
[222] *Id.* at 26.

https://doi.org/10.59015/wilj.KLCM3237

precautions in order to protect civilian populations from harm caused by a cyberattack on commingled facilities. These states are obligated to put in place safeguards, like segregating networks, setting up firewalls and intrusion detection systems, setting up access control and authentication, input patch management, holding security monitoring and logging, implementing vendor risk management, and maintaining continuous improvements, to protect nuclear facilities from cyberattacks on the malware development facilities. By implementing these protections, states protect their citizens from the effects of such attacks and will be in compliance with their obligations under Article 58 of Additional Protocol I.

https://doi.org/10.59015/wilj.KLCM3237