Nuclear Weapons, Cyber Warfare, and Cyber Security: Ethical and Anticipated Ethical Issues

Richard L. Wilson[1] and Alexia Fitz[2]
[1] Towson University, Towson, MD
[2] Towson University, Towson, MD

wilson@towson.edu
afitz2@students.towson.edu

Abstract: In this paper, we discuss the interrelationship of nuclear weapons, cyber warfare, and cyber security. Some of the most significant cyber threats to nuclear stability are now due to the intersection of technologies related to nuclear weapons and cyber technology. Cyber warfare can now be used to engage in and influence international events through cyber attacks upon nuclear systems and weapons. In the current war between Russia and Ukraine there has been the threat of the use of nuclear weapons. Since cyber warfare has already been employed in the Russia/Ukraine conflict it is possible that cyber attacks could be employed to trigger a nuclear event. To prevent cyber warfare from leading to nuclear warfare there needs to be a focus on cyber security in order to protect nuclear systems and nuclear arsenals but also to mitigate cyber attacks that could lead to the use of nuclear weapons. One of the main risks to nuclear weapons systems is sabotage. It is easy to imagine cyber attackers placing incorrect information into systems and even taking control of nuclear weapons. Various parts of nuclear weapons systems are capable of being targeted. Command and control systems, alert systems, launch systems, and target-positioning systems could all become targets. Scenarios in which alert systems are hacked and show a nuclear attack by adversaries, may lead to an accidental nuclear conflict. It is also conceivable that hackers could manipulate the coordinates of (pre-programmed) targets of nuclear missiles, or to spoof GPS-like systems that some missiles use to calculate their positions their targets. At the present time there is no evidence that any state or non-state actor is able to successfully perform such manipulations but considering the exponential rate of developments in the cyber arena, in the near future, such attacks might be possible. In the worst-case scenarios, these possibilities could lead to the inadvertent use of nuclear weapons, and/or use against unintended targets. In less dramatic scenarios, the perceived vulnerabilities of the nuclear weapons systems may affect nuclear stability. This could lead to a decrease in the deterrent value of nuclear weapons. This could come about because potential adversaries may think they have options to manipulate these weapons when being used. It is difficult to forecast the effects of decreasing nuclear deterrence. This analysis will define a stakeholder framework for identifying the ethical and anticipated ethical issues with cyber warfare and nuclear warfare and relate these issues to the importance of cyber security. Ethics should be at the center of the discussion of the use of nuclear weapons, nuclear warfare and cyber warfare. Moral concerns should be at the center of the discussion of nuclear warfare. The need for this moral concern is due to the threat to vulnerable populations by nuclear systems and nuclear weapons, as well as the threat posed to democratic institutions by the use of nuclear weapons.

Keywords: Nuclear Warfare, Nuclear Weapons Systems, Cyber Warfare, Cyber Security, Anticipatory Ethics

1. Introduction

The issues that link nuclear weapons, cyber warfare, and cyber security are directly related to the notions of strategy and tactics. In the political and military arenas when nuclear weapons are involved, strategy and tactics play an important role. Military strategy, in nation state to nation state confrontations, is a major concern and focuses on how forces may be deployed against one's armed opponents. Strategy involves the planning, coordination, and general direction of military operations to meet a nations overall political and military objectives. Military strategy can be contrasted with military tactics. Tactics are involved with implementing strategy by short-term decisions on the movement of troops and employment of weapons on the field of battle. In discussions of traditional warfare, security can be thought of as developing, planning and coordinating military operations in order to protect one's nation. Once a conflict between nations commences, tactics implement a nation's strategy by the movement of troops and the deployment of weapons. Both nuclear weapons and technologies employed as weapons, and cyber technologies used for conducting cyber warfare, present challenges for traditional conceptions of strategy and tactics. An important reason for this is related to the differences of scale between weapons and conventional weapons and the complexity nuclear warfare and cyber warfare when they are used in conjunction. These challenges are evident at 3 levels. First, there is the issue of what is meant by nuclear strategy and what is meant by strategy in the context of cyber warfare? Second, what is meant by tactics in the context of nuclear strategy and warfare, and what is meant by tactics in the context of cyber warfare? Third, how is security to be understood in the context of political and military strategies and tactics as they relate to nuclear warfare and cyber warfare? These questions are central to the ethical and anticipated ethical issues with nuclear weapons, cyber warfare, and cyber security. Ethics is concerned with

principles that govern a person's behavior or the conducting of an activity. In the context of nuclear weapons, cyber warfare, and cyber security the stakeholders involved in ethical thinking about warfare and foreign policy, takes place within nations and between adversaries, and thoughts are directly related to intentions, actions, and outcomes related to each of these subjects which need to be identified in order to identify ethical issues with the use of nuclear weapons, cyber warfare, and cyber security.

2. Nuclear Warfare

The threat of nuclear warfare since the first of such weapon's, has been related to political strategy, and to the potential for the deployment of nuclear weapons. Nuclear weapons are weapons of mass destruction, which contrast with weapons employed in conventional warfare. Nuclear weapons are much more powerful and destructive in a much shorter time than conventional weapons and can have a long-lasting effects such as effects related to radiation. A major nuclear exchange would probably long-term effects, primarily from the radioactive fallout released by detonation, and could also potentially lead to secondary effects, such as nuclear winter, problems with famine, and the collapse of societies. Thermal thermonuclear war with Cold War-era stockpiles, or even with the current smaller stockpiles, may lead to various negative scenarios including the potentiality of extinction for the human race.(See: 7 Possible Toxic Environments Following a Nuclear War – The Medical Implications of Nuclear War 1985 – The National Academies Press. 1986.)

After the Soviet Union dissolved in 1991 and after the end of the Cold War, the threat of a major nuclear war between the U. S. and Russia have been considered to have lessened. More recently, concern over nuclear weapons has altered to the prevention of localized nuclear conflicts resulting from nuclear proliferation and the threat of terrorists getting access to nuclear devices. However, the threat of nuclear war is considered to have resurged due to the war in Ukraine, and threats by Russia to use nuclear weapons in the conflict. (Could the war in Ukraine go nuclear?". *The Economist*. 2022)

3. Effects of Nuclear Warfare

Nuclear warfare where nuclear weapons are employed produce a number of effects. The effects of a nuclear detonation on the environment are much more destructive and multidimensional than those caused by conventional weapons. The energy released from the detonation of a nuclear warhead detonated within the lower part of the earth's atmosphere can be approximately divided into four basic categories: (See: The Effects of Nuclear Weapons)

- The energy released in the blast itself: 50% of total energy
- There is the release of thermal energy: 30–50% of total energy
- Ionizing radiation is released: 5% of total energy
- Residual energy is also released: 5–10% of total energy with the mass of the explosion.

Depending on the design of a particular nuclear weapon, and the location in which it is detonated, the energy distributed to a target can vary. The environment of the explosion plays a large role in determining how much energy is distributed to the blast and how much to radiation. (See: The Effects of Nuclear Weapons).

3. Cyber Warfare

In nation state to nation state conflicts, cyberwarfare can be considered to be the use of cyberattacks against an enemy state, with the intention of creating damage that is similar to the damage created by conventional warfare. A cyberattack would be aimed at disrupting vital computer systems. In the context of this analysis the attacks would be aimed at disrupting nuclear systems and nuclear weapons including the detonation of a target nation's nuclear arsenal.

There is a debate among experts concerning the definition of cyberwarfare, and whether cyberwarfare exists. A number of nations in the international community including the U. S., the United Kingdom, Russia, China, Israel, Iran, and North Korea have extensive cyber capabilities for both offensive and defensive cyber operations. As more nation states develop the use of cyber operations and combine capabilities such as combining cyber and nuclear weapons, the likelihood of kinetic confrontation and violence developing as a result of the combination of cyber operations and nuclear operations is likely to increase.

What could be the first example of a kinetic military action which was used in response to a cyber-attack and that involved the loss of human life occurred on 5 May 2019. The attack attributed to the Israel Defense Forces targeted and destroyed a building associated with an ongoing cyber-attack (see: Newman, Lily Hay (6 May 2019). "What Israel's Strike on Hamas Hackers Means For Cyberwar"),

4. The potential effects of cyber warfare on nuclear warfare

There has been a great deal of discussion of nuclear weapons and Related Systems and how they are Increasingly Vulnerable to Cyberattack. **A** Nuclear Threat Initiative (**NTI) report (see:** https://www.nti.org/news/new-report-finds-nuclear-weapons-and-related-systems-increasingly-vulnerable-cyberattack/) has found that there are significant cyber threats to nuclear weapons and related systems—including nuclear planning systems, early warning systems, communication systems, as well as delivery systems. These cyber threats include an increase in the risk of unauthorized use of a nuclear weapon, an increase in the risk of nuclear weapons as a result of false warnings, and the undermining of confidence in the development of nuclear weapons as a deterrent. These threats are made possible by the speed, stealth, unpredictability, and challenges related to attribution with cyberattacks, all of which make it difficult to anticipate, deter, and defend against all cyber threats.

The NTI report also identifies the implications of these cyber threats to nuclear weapons, while making recommendations that governments need to employ to mitigate the threats that cyberattacks pose to nuclear weapons systems and nuclear weapons. These recommendations are stated in the report include:

- Developing options for increased decision time to account for threats to early warning systems
- Establishing norms that would restrict cyber weapons use against nuclear weapons systems
- Enhancing survivability and resilience of nuclear systems and command, control, and communications systems
- Securing and diversifying critical systems
- Prioritizing addressing cyber risks in modernization plans
- Maintaining teams of experts
- Enhancing security of nuclear weapons, and reviewing the vulnerabilities of nuclear weapons to combined physical and cyberattacks
- Initiating bilateral dialogue with Russia
- Increasing international cooperation to reduce the cyber threat.

5. Cyber Security

The previous recommendations made within the NTI report all point to the need for an increase in cyber security related to the risks of cyber warfare being used against nuclear systems and nuclear weapons. Computer security, cybersecurity (cyber security), or information technology security (IT security) are all concerned with the protection of computer systems and computer networks from attacks by adversarial and malicious actors. These attacks may result in the accessing protected information, theft of information or data, and damage to computer hardware and software. Cyberattacks could lead to the disruption and r misdirection of the services provided by computer networks. The threats posed by these types of cyberattacks to nuclear systems and nuclear weapons show the need for cyber security in these domains.

Cyber security has increased in importance as the result of the continual development and reliance on computer networks, the use of the internet and wireless network technologies. The continued development of technologies capable of connecting to the internet including Wi-Fi, Smart Devices, Smartphones and every device capable of being connected to the Internet of Things have lead to the interconnection of everything including nuclear systems and nuclear weapons. Cyber security faces significant difficulties for all aspects of the contemporary world, due to the reliance upon computer and information systems and the complexity of these systems. Cyber security is of significant important for systems that govern large-scale systems such as nuclear systems and nuclear weapons. The devices that connect to the emerging internet of things introduce multiple attack vector that could be employed to attack nuclear systems and nuclear weapons.

6. Nuclear Warfare, Cyber warfare and Cyber Security

There are a number of dangers that lead to the need for cyber security in the domains of nuclear warfare and cyber warfare. **Nuclear systems and weapons can be hacked.** Nuclear and information computer technology professionals are aware that all digital computer systems are at risk for cyberattacks which includes nuclear

weapons systems and nuclear weapons. This also means that any nation state that has warheads, delivery vehicles, and the technology used to control them, are capable of becoming prime targets and that they are vulnerable to cyberattacks and hacking. The defense systems relied upon to detect incoming attacks are also vulnerable. These same cyber vulnerabilities are in nuclear weapons systems and undermine the safety and security of nuclear weapons around the world.

The problem is that a successful cyberattack on a nuclear weapon system could result in nuclear detonation or even cause an all-out nuclear war. There are a number of ways that cyber threats could increase the chance of miscalculation and lead to nuclear use in the U.S.-Russia or Ukraine- Russia context (adapted from "The Cyber nuclear Threat" https://www.nti.org/analysis/articles/cyber/#:~:text)

1. Malicious actors are capable of interfere in U.S. or Russian or any nation's nuclear command and control systems.
2. Hackers could spoof the U.S. or Russian or any nations early warning system, leading either country to believe they're under attack.
3. A cyberattack on a communication system or nuclear systems and weapons could render the United States or Russia or any nation, unable to ensure that their nuclear weapons remain under proper control.

The vulnerability problem isn't confined to the use of nuclear weapons by the United States or Russia. Nine countries have nuclear weapons, and if these systems were compromised this creates a global nuclear risk.

7. Strategies for cyber security against cyber warfare on nuclear weapons

In another Nuclear Threat Initiative (NTI) report (Addressing Cyber-Nuclear Security Threats, see: https://www.nti.org/about/programs-projects/project/addressing-cyber-nuclear-security-threats/) a number of issues are presented related to cyber warfare and nuclear weapons. Important questions arise when we consider what kind of cyber threats could occur which are directed at nuclear systems and nuclear weapons. What would happen if a cyberattack shut down the security system at a highly sensitive nuclear materials storage facility, giving access to terrorists seeking highly enriched uranium required to make a bomb? Hackers could spoof a nuclear missile attack, which could trigger a miscalculated retaliatory strike that could kill millions.

The threat of cyberattacks can affect the nuclear risk environment in at least two ways: cyberattacks can be used to undermine the security of nuclear systems including the safety of nuclear materials and facility operations, and cyberattacks can compromise nuclear command and control systems for nuclear weapons. According to the NTI report nuclear security practices have in the past focused on preventing physical attacks—this means employing "guns, guards, and gates" to prevent 1) theft of materials to build a bomb, 2) sabotage of a nuclear facility, or 3) unauthorized access of nuclear command, control, and communications systems. Progress has been made in these areas, however the threat of a cyberattack against nuclear control systems and weapons is escalating. Nuclear cybersecurity practices need to be brought up to date with regard to the extend of current risks. The threat's to nuclear systems extends to the command, control, and communications (NC3) for nuclear weapons. Cyber threats are becoming increasingly sophisticated as information technology continues to develop and those responsible—from policymakers to military officials to facility operators to regulators have to continually work to keep up with these developments. There is a need to develop a set of guiding principles for cybersecurity at nuclear facilities. The current mindset needs to be replaced with the idea that there are ever-evolving threats to nuclear systems and nuclear weapons. An overarching framework that guides cybersecurity at nuclear facilities is needed.

8. BDI Model and Nuclear Cyber Security

The BDI model will serve as the foundation for understanding how actors involved in nuclear warfare, cyber warfare and cyber security are related to one another and eventually the distinctions from the BDI model can be employed to discuss how ethical issues emerge. What is BDI model? The Belief-Desire-Intention (**BDI**) **model** of human practical reasoning, developed by Michael Bratman (1987), is a model for assessing the rationality of human actions. The BDI model introduces future-directed intentions, which are composed to plans, as an important and irreducible concept. In the agent research community, the BDI model has been slightly adapted to specify the behavior of software agents in terms of beliefs, goals and plans. (Bratman, Intention, Plans, and Practical Reason). The model is diagrammed below.

Beliefs
→ intention → action → outcome
Desires

The BDI model plays an important role in predicting how agents will act and can also serve as the basis for predicting how agents will act, as well as for helping to predict how future directed reasoning will occur in practical reasoning which is directed towards achieving future goals. This model is used to predict the behavior of others while at the same recognizing we can apply the model to ourselves. The model can be employed to clarify how we develop our plans in order to attempt to achieve our goals. These beliefs and desires are the basis of intentions, actions and goals.

How can this model apply to nuclear weapons, cyber warfare, and cyber security? We will focus on political and military leaders in this preliminary analysis. There are nation states and political and military agents within them, who entertain the idea of nuclear war. These agents have beliefs and desires, they also have intention's and they have goals. There are agents who entertain the idea of cyber war. These agents who have beliefs and desires, they have intentions, and they have goals. There are agents who entertain the idea of cyber security. These agents who have beliefs and desires, they have intention's and they have goals. Adversaries in nuclear war and cyber war have beliefs and desires, they have intentions. and they have goals. As adversaries these are all capable of being at odds with one another. Security and Cyber security attempt to mitigate for example the intentions of adversaries to use nuclear warfare and cyber warfare against one another.

9. BDI Model and Ethics

How can the BDI model be related to ethics? For the purposes of this analysis we will remain focused on standard principles with philosophical ethics. Any number of principles could be employed for conducting an ethical analysis by relating them to an actor's intentions, actions and projected goals but here we will relate them to standard principles with philosophical ethics. Ethics in a basic definition relates to agents who perform actions. Dwight Furrow identifies and expands upon the focus of ethical analysis as involving a series of factors. As Furrow states, ethics is related to evaluating actions and actions are performed by those capable of being moral agents. Furrow continues by stating, "When we evaluate an action, we can focus on various dimensions of the action. We can evaluate the person who is acting, the intention or motive of the person acting, the nature of the act itself, or the consequences." (Furrow, Ethics: Key Concepts in Philosophy)

Two points are made within this passage. Ethical issues related to situations and cases are based upon the idea that when agents perform actions, these actions are capable of moral assessments. Moreover, actions are an extension of what a person does when they deliberate upon possibilities. In other words, the actions of agents are capable of being evaluated based upon both the intentions and actions of the person involved in the situation or case. If this is true and if we endorse the distinctions identified in the preceding passage and apply them to the assessment of moral responsibility in situations and cases, there are three levels of moral responsibility and evaluation. We can evaluate the actions of a person in the situation or case, we can assess the intentions of the persons involved in the situation or case, and we can assess the consequences of the actions intended by the person in the situation or case.

In order to understand the ethical issues involved with nuclear weapons, cyber warfare, and cyber security through situations and cases, we need to have an additional understanding of ethics and moral responsibility. Part of the difficulty related to ethical analysis requires the identification of what ethical principles to employ in our ethical analysis. Here we can only point to how this analysis would proceed.

Below is a preliminary diagram showing how ethical principles can be adjoined to Bratman's BDI model.

beliefs
goals
Character Traits Intentions → Actions → Outcomes
Virtue Ends
Ethics ↓ ↓
Desires

Deontology Consequentialism

Aristotle Kant and Ross Mill

Some Feminist
Ethicists

The distinctions on this diagram can be applied to the distinctions made above. Adversaries in nuclear war and cyber war have beliefs and desires, they have intentions, and they have goals. As adversaries they are capable of being at odds with one another. Security and Cyber security attempt, for example, to mitigate the intentions of adversaries to use nuclear warfare and cyber warfare against one another. Adversaries in nuclear war and cyber war have intentions (that violate or support rules and duties) and they have goals (that if achieved produce positive or negative consequences). A detailed ethical analysis apply ethical principles to each stakeholder perspective affected by nuclear weapons, cyber warfare, and cybers security.

10. Anticipatory Ethics

According to Phillip Brey (see: Anticipatory Ethics for Emerging Technologies, 2012) anticipatory ethics is concerned with examining ethical issues that arise from the emergence of technologies. This focus is particularly important due to the increasing rate at which technological developments are taking place. There is also an additional element that is important in this discussion, technologies not only continue to develop at a rapid rate, they are also converging with one another at a rapid rate. The focus of this analysis nuclear weapons, cyber warfare, and cyber security highlights difficulties related to the developments of technologies in all of these areas. While there are technical issues and ethical issues with developments in each of these areas, there are also technical and ethical issues due to the convergence of these 3 areas. New technologies are created when disparate technologies converge. Anticipatory ethics is an important method for attempting to identify ethical problems and potentially emerging ethical problems that might occur when technologies converge.

The convergence of nuclear warfare, cyber warfare and cyber security present a number of difficulties related to intentions, actions and outcomes that adversaries can employ against one another. However, a thorough anticipatory ethical analysis would seem to require much more than an analysis of the viewpoints of adversaries in a conflict. There are a wide variety of stakeholders who would be affected by any use of a nuclear weapon. These stakeholders would include political leaders, military leaders, deployed soldiers, designers of weapons, builders of weapons, individuals in the area where a nuclear weapon has been deployed, medical personnel, and global individuals. This is at best an extremely partial list of stakeholders who would be affected by the use of a nuclear weapon. The complexity of ethical issues becomes larger when we construct a list of stakeholders affected by cyber warfare and then move on to construct a stakeholder list of those involved with cyber security. Finally, a list of stakeholders needs to be constructed that identifies those affected when nuclear, cyber warfare and cyber security technologies converge. In all of these arena's we contend that actors have all of the items referred to in the BDI model. Actors have beliefs and desires, they have intentions, they perform actions, and they have goals that are aimed at producing outcomes. The ethical issues that emerge are related to how the stakeholders involved in nuclear weapons, cyber warfare, and cyber security are related to one another. The intention to employ nuclear weapons in an armed conflict can be examined from each stakeholder perspective. The decision can be examined from the perspectives of politicians, military leaders or civilians potentially affected by the use of nuclear weapons. Ethical issues and responsibilities can be identified from each stakeholder perspective.

11. Conclusions

Due to length constraints we now need to narrow our analysis to 2 stakeholder perspectives, political and military leaders. When considered from the stakeholder perspective of politicians/military leaders, nuclear warfare and the use of nuclear weapons presents a number of advantages and disadvantages for issues for political and military adversaries that would affect their intentions, actions and goals.

The advantages of nuclear weapons include (adapted from 17 Advantages and Disadvantages of Nuclear Weapons)

1. **From a border-based perspective they reinforce the idea of nationalism.**
2. **Nuclear weapons serve as a deterrent to a global conflict.**
3. **Nuclear weapons technology creates a bargaining chip for countries that need it.**
4. **Nuclear weapons reduce the threat to a country's military forces.**
5. **Governments can position nuclear weapons in a variety of launch locations.**

6. **Nuclear weapons research has contributed to the creation of new technologies in other sectors.**
7. **The reliability of nuclear weapons is one of its greatest attributes.**

When considered from the stakeholder perspective of politicians/military leaders nuclear warfare presents a number of issues for adversaries that are also disadvantages.

1. **There will always be moral and ethical debates about the use of nuclear weapons.**
2. **Nuclear weapon detonations are directly connected to cancer development.**
3. **There are direct costs attributed to a government's nuclear weapons program.**
4. **Nuclear weapons devastate the environment.**
5. **The use of nuclear weapons creates a significant threat of terrorism.**
6. **The development of nuclear weapons creates hazardous waste.**
7. **Degraded delivery systems can cause a nuclear weapon to fail.**
8. **We create nuclear weapons from non-renewable resources.**
9. **It requires a specific skill set to develop or maintain nuclear weapons.**
10. **Everyone is still dealing with the after-effects of nuclear weapons testing.**

When we examine the advantages and disadvantages of nuclear weapons, the idea of a threat deterrent does not seem to aim at genuine peace. The development of nuclear weapons is a race to create something bigger or more defensive in an weapons development program is not aimed at ending the threat of nuclear war. The use of significant conventional weapons without the threat of nuclear detonation and radiation exposure and the severe loss of civilian life, would perhaps be a better way of achieving the same goals. If we approach the issue of the dangers of nuclear weapons from the perspective of the convergence of nuclear weapons, cyber warfare and cyber security, we can see that Cyber warfare presents a number of possible attack vectors for attacking all adversaries with nuclear weapon systems, nuclear weapons and cyber warfare.

In the case of nuclear warfare we now assume that we can use the distinctions referenced by Furrow that focus on the actions of agents and we can state that adversaries are concerned in terms of intentions, actions, and outcomes with exploiting all the weaknesses of adversaries. What anticipatory ethics must focus on is mitigating are the intentions, actions and outcomes aimed at by adversaries when nuclear warfare and cyber warfare are thought about together. Here we will focus on Cyber Security as the basis for accomplishing this mitigation. **The spread of new cyber capabilities combined with the increasing digitization of nuclear systems increases the likelihood of dangerous cyber-nuclear attacks focused on nuclear systems and nuclear weapons. (See: The Cyber Nuclear Threat,** https://www.nti.org/analysis/articles/cyber/#:~:text=**)**

The United States as well as other countries with nuclear systems and nuclear weapons, are concerned with outdated technologies that need to be replaced by modern digital components as part of broad nuclear modernization programs. However according to the U.S. Government Accountability Office, at least in the United States, these technologies could create more problems than they solve: there are "mission critical cyber vulnerabilities" in nearly all the weapons systems under development by the Department of Defense. (See: Nuclear Weapons Cybersecurity: NNSA Should Fully Implement Foundational Cybersecurity Risk Management Practices, https://www.gao.gov/products/gao-22-104195)

Due to these difficulties according to the GAO Cybersecurity Risk Management Practices need to be put into effect. According to the GAO analysis these practices include:

1. Cybersecurity roles and responsibilities for risk management need to be identified.
2. Organizations need to establish maintain and review risk management strategies for nuclear weapons systems.
3. Policies and plans for the cybersecurity program need to be documented and maintained.
4. Organization wide cybersecurity risks need to be assessed and updated
5. Designate controls that are available for information systems or programs to inherit.
6. Strategies for continually monitoring risks need to be developed and maintained across organizations.

Finally due to insights provided by the discovery of Solar Winds, Cybersecurity Risk Management Practices also need to be implemented in numbers of arenas. These areas include: (See: Nuclear Weapons Cybersecurity: NNSA Should Fully Implement Foundational Cybersecurity Risk Management Practices, https://www.gao.gov/products/gao-22-104195).

The **operational technology environment which** includes sub-contractors who manufacture equipment and who build control systems with embedded software to monitor physical devices or processes needs to be made cyber secure.

The **nuclear weapons IT environment** including IT in or in contact with weapons. NNSA has implemented or taken action consistent with implementing most of the practices in this environment and is developing specific guidance for contractors needs to be made cyber secure.

NNSA's cybersecurity directive requires contractors to oversee their subcontractors' cybersecurity measures, but contractors' efforts to provide such oversight are mixed, and three of seven contractors do not believe it is a contractual responsibility. The recommendation is that contractor and cub contractor environments need to be made cyber secure.

In addition to identifying the risk factors listed above, which involve technical issues related to risks for nuclear systems, nuclear weapons and cyber warfare, a thorough ethical and anticipatory ethical analysis would also need to identify all of the stakeholders potentially affected by nuclear weapons, cyber warfare, and cyber security. The difficulty of this task is related to the intentions, actions and goals of all of the stakeholders involved. Ethical issues for each stakeholder are related to their intentions, actions and outcomes. Ethical problems emerge when stakeholder intentions, actions and outcomes clash with other stakeholder intentions, actions and outcomes on important issues. This ethical analysis will require a sustained analysis of situations and cases related to stakeholder involvements with nuclear weapons, cyber warfare, and cyber security. Here we merely outline this extensive project. Here we have only outlined some of the problems that will require a much more extensive analysis. This will carried out in future analysis and research.

References

17 Advantages and Disadvantages of Nuclear Weapons, Future of Working, https://futureofworking.com/6-advantages-and-disadvantages-of-nuclear-weapons/.

Ackerman, Pascal. Industrial Cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment, 2nd Edition 2nd ed., Packt Publishing; 2nd ed. edition (October 7, 2021).

"Addressing Cyber Nuclear Threats", Nuclear Threat Initiative 2022, https://www.nti.org/about/programs-projects/project/addressing-cyber-nuclear-security-threats/.

Bratman, Michael. Intention, Plans, and Practical Reason, Center for the Study of Language and Information; New edition (March 1, 1999).

Brey, Phillip. Anticipatory Ethics for Emerging Technologies, Nanoethics, 6 (1):1-13 (2012).

"computer security | Definition & Facts | Britannica". *www.britannica.com*. Retrieved 12 July 2022.

Could the war in Ukraine go nuclear?". *The Economist*. Sept 29. 2022. https://www.economist.com/international/2022/09/29/could-the-war-in-ukraine-go-nuclear.

Cunningham, Chase. Cyber Warfare – Truth, Tactics, and Strategies: Strategic concepts and truths to help you and your organization survive on the battleground of cyber warfare, Packt Publishing (February 25, 2020)

Ehrlich, P. R.; Harte, J.; Harwell, M. A.; Raven, P. H.; Sagan, C.; Woodwell, G. M.; Berry, J.; Ayensu, E. S.; Ehrlich, A. H.; Eisner, T.; Gould, S. J.; Grover, H. D.; Herrera, R.; May, R. M.; Mayr, E.; McKay, C. P.; Mooney, H. A.; Myers, N.; Pimentel, D. & Teal, J. M. (1983). "Long-term biological consequences of nuclear war". *Science*. **222** (4630): 1293–1300.

Fitz, Alexia and Richard L. Wilson. **Just Warfare: Is a Nuclear Attack an appropriate Response to a Cyber Attack? Forthcoming in the proceedings for the** 18th International Conference on Cyber Warfare and Security 9 - 10 March 2023, Towson, Baltimore County, Maryland, USA.

Furrow, Dwight. Ethics: Key Concepts in Philosophy, Continuum, New York, NY. 2005.

Huskaj, Gazmend and Richard L. Wilson. **HUSUSUSKAJ, GUZMANDOFFENSIVE CYBERSPACE OPERATIONS AND ZERO-DAYS: ANTICIPATORY ETHICS AND POLICY IMPLICATIONS FOR VULNERABILITY DISCLOSURE,** JOURNAL OF INFORMATION WARFARE, VOL 20, ISSUE 1, 2019.

Huskaj, Gazmend and Richard L. Wilson. **Anticipatory Ethics for Vulnerability Disclosure, published in the proceedings of the 18th European Conference on Cyber Warfare and Security, Dayton, Ohio, 2019.**

Lin, Herbert. Cyber Threats and Nuclear Weapons, Stanford University Press; 1st edition (October 19, 2021).

Lucas, George. Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare, Oxford University Press; 1st edition (December 13, 2016).

Martin, Brian (December 1982). "The global health effects of nuclear war". *Current Affairs Bulletin*. **59** (7).

Newman, Lily Hay (6 May 2019). "What Israel's Strike on Hamas Hackers Means For Cyberwar" Wired, https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/.

"Nuclear Explosions: Weapons, Improvised Nuclear Devices". U.S. Department of Health and Human Services. 16 February 2008.

"Nuclear Weapons Cybersecurity: NNSA Should Fully Implement Foundational Cybersecurity Risk Management Practices". 2022, https://www.gao.gov/products/gao-22-104195.

Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". *Journal of Digital Forensics, Security and Law*. **12** (2).

Schnur and Richard L. Wilson. Cold War Echoes: The Russian Effort to Interfere in the 2016 Election, published in the proceedings of the 13th International Conference on Cyber Warfare and Security, Dayton, Ohio, 2017.

Stoutland, Page O. PhD and Samantha Pitts-Kiefer. Nuclear Weapons In the New Nuclear Age, 2018. https://www.nti.org/wp-content/uploads/2018/09/Cyber_report_finalsmall_Zg5TarX.pdf.

Stoutland, Page O., Addressing Cyber-Nuclear Security Threats, 2022. https://www.nti.org/about/programs-projects/project/addressing-cyber-nuclear-security-threats/.

"The Cyber-Nuclear Threat", Nuclear Threat Initiative 2022, https://www.nti.org/analysis/articles/cyber/#:~:text.

The Effects of Nuclear Weapons, https://www.britannica.com/technology/nuclear-weapon/The-effects-of-nuclear-weapons.

"The Energy from a Nuclear Weapon". *www.atomicarchive.com*.

What is BDI Model. IGI Global Publisher of Timely Knowledge. https://www.igi-global.com/dictionary/bdi-model/2286,/.

Wilson, R. L. (2021, April), *Anticipatory Ethics as a Method for Teaching Engineering Ethics* Paper presented at 2021 ASEE St. Lawrence Section Conference, Virtual. Now in the ASEE proceedings at: https://peer.asee.org/38292 .

Wilson, Richard L. State Sponsored Information Deception, Social Media, and the Rise of 'Soft' Warfare, presented at the 13th International Conference on Cyber Warfare and Security, Dayton, Ohio, 2017.

Wilson, Richard L. State Hacktivism, Cyber Warriors and Cyber Warfare, presented at the 13th International Conference on Cyber Warfare and Security, Dayton, Ohio, 2017.