UVU Security Review

Volume VIII   Issue I

Spring 2023

UVU Security Review

The *UVU Security Review* is Utah's first student-edited academic journal focused on national security issues. The *Review* is published twice annually—in April and December—and it is supported by the Center for National Security Studies (CNSS) at Utah Valley University (UVU). The *Review* publishes timely, insightful articles on critical national security matters, including topics relating to foreign affairs, intelligence, homeland security, terrorism, and national defense. The *Review* accepts articles from UVU students, alumni, faculty, staff, and administration. Submissions should be sent to the *Review* Editor-in-Chief at CNSS-Journal@uvu.edu.

The Center for National Security Studies

The CNSS at UVU was established in January 2016. The Center is the first of its kind in the State of Utah. The CNSS is a nonpartisan academic institution for the instruction, analysis, and discussion of issues related to the field of US national security. The mission of the CNSS is twofold: to promote an interdisciplinary academic environment on campus that critically examines both the theoretical and practical aspects of national security policy and practice; and to assist students in preparing for public and private sector national security careers through acquisition of subject matter expertise, analytical skills, and practical experience. The CNSS aims to provide students with the knowledge, skills, and opportunities needed to succeed in the growing national security sector.

Utah Valley University

UVU is a teaching institution that provides opportunity, promotes student success, and meets regional educational needs. UVU builds on a foundation of substantive scholarly and creative work to foster engaged learning. The university prepares professionally competent people of integrity who, as lifelong learners and leaders, serve as stewards of a globally interdependent community.

The opinions expressed in this journal are the views of the authors and do not necessarily reflect the views or opinions of Utah Valley University.

CONTENTS

UVU Security Review

Volume VIII   *Spring 2023*   *Issue I*

A Note from the Editor-in-Chief

I have been extremely grateful to work on the *UVU Security Review* this semester. It was an honor to be asked to lead this publication. I have had opportunity to reach out to many renowned practitioners in the security field and it broadened my horizons; these authors write about so many different topics, but all are of extreme importance to our society. These thought-provoking pieces will bring great discussion and information to those reading.

I would like to thank the many people who have worked with me to help this journal be what it is today. To my executive editor, Brenton Rasmussen, and managing editor, Michelle Stanley, along with my content editors, thank you for your time and effort in helping support this journal. Thank you to Deb Thornton and her team of editors, who spent so much of their time and energy on helping source check and edit. This truly would not have been possible without each and every one of you. Thank you to faculty member, Mike Smidt, who assisted me in finding wonderful authors to publish and guiding the journal to where it is today.

Publishing the *UVU Security Review* is an experience I will never forget, and I am forever appreciative of the time I had and the people I met during this process. I hope every reader is able to enjoy this edition as much as I have.

Alysa Warlin
Editor-in-Chief

Automated Weapons Systems, Accountability, and Responsibility

Hope Fager

Today's world is consistently challenging what we thought we knew about technology. As time passes, what standard computers are able to do with simple ones and zeroes is growing exponentially. One of the most prominent examples of this growth is Artificial Intelligence (AI) and its wide range of applications. Such examples include simple recommendations online, where algorithms make suggestions on purchases or media. In these cases, a misjudgment on the part of the AI would simply result in a user ignoring the recommendation, or even choosing to click "don't show me this again." Other commercial uses of AI have grown in their abilities exponentially, with facial recognition capabilities, deep fakes, and other potentially damaging uses.

However, there are higher stakes in the military applications of AI, such as Automated Weapons Systems (AWS). For this reason, many people, including the United States Department of Defense, agree that humans should always be involved in the judgement and decision-making process when using AWS following the International Law of Armed Conflict and the Rules of Engagement. This policy, of course, is for accountability purposes. If an AWS ever is used to commit a war crime, then the person doing so can be held legally accountable for the action. The more difficult question comes into play when the weapon is not necessarily being operated by a human, but being supervised, or even being left to make its own decisions. An AWS cannot be held accountable itself for incorrect or illegal targeting the way a person can be, so, who can? The manufacturers, the writers of the code, the people who tested the product for reliability, the officers in the military that approved its use, the soldier using the weapon in that particular instance? To what extent can each of these parties be held accountable? While humans and states must always be accountable for the actions of AWS, it is vital that international law define and classify AI and AWS in order to maintain accountability even in the future when AWS are completely independently deployed.

Classification of Autonomous Weapons Systems

Different types of AWS are distinct from each other based upon their level of autonomy from human input or intervention. The Department of Defense Directive number 3000.09 specifies definitions for AWSs, named "autonomous weapons systems," "human-supervised autonomous weapons systems," and "semi-autonomous weapons systems".[1]

Autonomous Weapons Systems

AWS are defined in the directive as

> "a weapons system that, once activated, can select and engage targets without any further intervention from a human operator. This includes human-supervised auto nomous weapons systems that are designed to allow human operators to override operation of the weapons system, but can engage and select targets without further human input after activation."[2]

A general AWS is any weapon that can select and engage targets independently without any human intervention. This also includes AWS that takes any input from humans, including identified targets or the cancellation of engagements.

Human Supervised Autonomous Weapons

Human supervised autonomous weapons systems are similarly defined in the same directive as "an autonomous weapon system that is designed to provide human operators with the ability to intervene and eliminate engagements, including in the event of a weapon system failure, before unacceptable levels of damage occur." [3] This type of AWS is capable of automatically choosing and engaging its own targets based on input data. An operator can cancel any engagement that the AWS may choose, but if there is no intervention on the part of the operator, the AWS works independently.

Semi-Autonomous Weapons

Semi-autonomous weapons systems are also presented in the directive as “a weapon system that, once activated, is intended to only engage individual targets or specific groups that have been selected by a human operator.”[4] This type of AWS does not choose targets on its own, instead requiring that an operator pick a target for the weapon to independently engage.

Other Classifications

Classifying autonomous weapons systems is not unique to the Department of Defense. The NATO Office of Legal Affairs uses the OODA (Observe, Orient, Decide, and Act) decision loop system to define and classify autonomous weapons systems. They make the distinction that “an ‘in-the-loop’” system requires human intervention for its operation, an “‘on the loop’” system provides for human intervention if needed, and an “‘out of the loop’” system does not require human intervention at all”.[5] In this context, “‘in the loop’” systems are comparable to semi-autonomous weapons that require an operator to choose targets for them. This term is used because the operator is “in the loop” of the decision making. “‘on the loop’” systems are comparable to human-supervised autonomous weapons where the AWS chooses targets and engages them independently, and the operator has the ability to cancel the engagement. This term comes from the idea that while the operator is not “in the loop” making the decisions, they are “on the loop” supervising it. Finally, “out of the loop” AWS are truly autonomous and have no operator at all, and therefore humans are completely “out of the loop” of decision making.

Policy and International Law of Automated Weapons System Use

The DOD makes it very clear that “‘out of the loop’” automated weapons systems are not to be used by the United States military. It is specified that “autonomous and semi-autonomous weapon systems shall be designed to allow appropriate levels of human judgement over the use of force”[6] in DOD Directive 3000.09 (4)(a). This immediately rules out the use of true AWS as they do not allow for operator input or influence. It is also specified that “systems will go through rigorous software and hardware verification and validation . . . and realistic system developmental and operational test and evaluation”.[7] Later in the document it is also specified that “training, doctrine, and tactics, techniques, and procedures . . . will be established”, as well as requiring all weapons systems to be designed with "human machine interfaces and controls".[8] These three requirements are all designed to keep levels of operator autonomy in AWS usage. Verification and validation will ensure that the system operates as intended in whatever simulated battlefield situation is offered. Training and documentation of the system will allow operators to use the weapon effectively without unintended consequences. Finally, the presence of human machine interfaces will give operators the consoles required to give commands to the system.

All of the above is DOD policy, but there are very few laws that specify restrictions on the use of AWS. The International Committee of the Red Cross (ICRC), as recently as March 2022, has called on the Group of Governmental Experts to work "towards the adoption of new, international, legally binding rules".[9] This is in tandem with the ICRC recommendation to "prohibit autonomous weapons that are unpredictable and those designed or used to target humans".[10] This recommendation stems from the idea that autonomous weapons are 'victim activated' and therefore should be restricted. This would be the same way that landmines, which are also 'victim activated,' are restricted now.[11] However, these ICRC recommendations are not legally binding, and while they claim that "most High Contracting Parties, individually and jointly with others, have previously expressed their readiness to commit to not develop nor to use autonomous weapons that pose unacceptable risks and to commit to establish limits on all others",[12] international laws have yet to be adopted.

Some more traditional weapons laws can apply to autonomous weapons, coming primarily from the Additional Protocol I (AP I). Article 36 of AP I requires that

> "in the study, development, acquisition, or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or any other rule of international law applicable to the High Contracting Party."[13]

As a result, the employment of any and all weapons, including AWS must be able to follow the laws of armed conflict. In order for AWS to operate independently, they must be able to follow all these laws, including Articles 57 and 58 which do not mention autonomous weapons but still outline required precautions of attack including requirements for legal targeting.

Hypothetical Situations

In order to discuss accountability of AWS, this paper will use the following hypothetical situation. Intelligence suggests that a specific enemy car containing a high-ranking official will be travelling down a specific road in the middle of the night. Under the cover of darkness, a sniper looking down over the road. A car passes by, and the sniper recognizes the emblem painted on it to be that of the enemy, so he takes a shot and eliminates the driver of the car. Upon closer inspection however, the car was actually a civilian vehicle, and a particularly bent door looked like the enemy's emblem in the dim lighting. Per Article 85 (3) (a) of AP I, the sniper may have committed a grave breach of the Protocol.[14] The argument could be made that in this or similar cases, the sniper did not commit the crime willfully or that appropriate intelligence gave reason to assume the car was a legal target. Regardless, the sniper could be charged with a grave breach for killing a civilian.

Hypothetical with a Human Supervised Autonomous Weapons System

In a similar circumstance, instead of sending a sniper, the United Sates Army decides to use a human supervised autonomous drone to watch the area, guided by an enlisted soldier. Watching through the onboard camera, the soldier recognizes the emblem of the enemy on the car and highlights the target for the drone. Once given the target, the drone engages independently and fires on the driver. Once again, however, the car turns out to be a civilian vehicle, and the enemy emblem was actually a door bent out of shape in the dim lighting. This situation, once again, puts the charges of the potential crime onto the operator supervising the AWS. The operator was the one who chose the target and marked it for engagement. As in the last example, AP I Article 85 (3)(a) declares that making the civilian population or individual civilians the object of attack a grave breach of protocol.[15] Even though the human supervised drone was the one that fired, the human operator was the one that chose the target and made the drone engage the target.

Hypothetical with a Semi-Autonomous Weapons System

Finally, in a last circumstance, the same set up applies where intelligence reports that an enemy vehicle containing a high-ranking official will drive down a particular street on a specific night. However, this time, the United States Army launches a semi-autonomous drone with a human watching but not participating. The drone finds the car and uses its image recognition capabilities to identify the enemy emblem on the side of the vehicle. Independently, it engages the target and shoots the person in the driver's seat. While all this is occurring, the operator is watching the drone and the target chosen and chooses to let the drone engage rather than cancelling the engagement. As the car was actually civilian with a civilian in the driver's seat, the human who failed to stop the attack could be charged with the same crimes as stated above. While the human did not take the shot, or choose the target, he did fail to stop a breach of the protocol and therefore can still be charged per Article 86 of AP I.[16]

Human Accountability of Actions using Automated Weapons Systems

Questions have been raised about who is responsible for faulty actions of AI. Many different people and entities could be held partially accountable including the manufacturer, programmer, government representative that approved the use of the weapon in general, the military member who approved the use in the specific circumstance, or the operator overseeing the AWS in the moment. All of these have advantages and flaws, and accountability would have to be assigned after an investigation into the incident and the functionality of the AWS itself. If the manufacturer did not assemble the AWS properly, the accountability could fall at least partially on them. Similarly, a flaw in the coding of the AWS could fall on the programmer, an incorrect stress test could fall on the testers, and if officials approving the product ignored vital statistics, they would be accountable for doing so. In most cases however, if all the previous did not apply, the responsibility would fall on the operator (whether supervising or available to step in) and the state as a whole. AP I Article 87 (1) says that "military commanders, with respect to members of the armed forces under their command and other persons under their control, [are required] to prevent and where necessary to suppress and report to competent authorities breaches of the Conventions and of this protocol".[17] In addition to Article 87, Article 91 also reads "a party to the conflict which violates the provisions of the Conventions or of this Protocol shall, if the case demands, be liable to pay compensation. It shall be responsible for all acts committed by persons forming part of its armed forces".[18] NATO also reports that "the rules relating to State responsibility can inform discussions on defining the relationship and responsibility between human and machine in the use of AI-enhanced weapons".[19]

Such statements spur on regulations that governments and alliances have adopted in order to mitigate crimes as much as possible. In order to ensure that the principles of responsible use outlined in the NATO AI Strategy are met, very strict measures for development and testing of autonomous weapons systems are outlined. These include the principles of lawfulness, responsibility and accountability, explainability and traceability, reliability, and bias mitigation, as well as the responsibility of "[striving] to protect the use of AI from such interference, manipulation, or sabotage, in line with the Reliability principle in responsible use, also leveraging AI-enabled Cyber Defense applications."[20] The DOD directive 3000.09 also expands on this outlining strict and redundant methods of testing and requirements for safe development. This is further expanded on the U.S. Department of Defense Responsible AI Strategy and Implementation Pathway.[21] Despite all these strict guidelines over development of AI and autonomous weapons, the ICRC has recommended that "unpredictable autonomous weapon systems should be expressly ruled out, notably because of their indiscriminate effects" and "the use of autonomous weapon systems to target human beings should be ruled out".[22] The NGO Stop Killer Robots goes even further with this idea, recommending that AWS should not be used at all.[23]

While the idea of eliminating the use of autonomous weapons is not widespread, the idea that humans must be responsible for the actions of autonomous weapons systems is not anything new. The Department of Defense has required that all weapons have some sort of human intervention for accountability, and the ICRC has stressed that the issue with fully autonomous weapons is that "the use of autonomous weapon systems entails risks due to the difficulties in anticipating and limiting their effects. This loss of human control and judgement in the use of force and weapons raises serious concerns from humanitarian, legal and ethical perspectives".[24] The NATO AI Strategy agrees with this in the sense that one of the principles of responsible use is Responsibility and Accountability, "AI applications will be developed and used with appropriate levels of judgement and care; clear human responsibility shall apply in order to ensure accountability".[25]

These statements operate on the idea that human judgement is more reliable and more often correct than the judgement and decisions made by AWS and the AI that powers them. This is another main reason that the DOD uses such strict policies and principles relating to the use of AI and AWS. AI has not advanced to a point where it can be as reliable or as consistent as human judgement, and as a result, there is a current need for human operators to assist in the operations of the AWS.

System Accountability of Autonomous Weapons Systems

AI, and therefore AWS, is advancing at an incredible rate. While human judgement is more consistent and more reliable than AI at the moment, the day might not be far off where the gap between the two is small or almost nonexistent. While there is heavy debate on the ability of AI to ever become sentient, it would not have to actually become sentient to be able to make the right call consistently enough to be left without an operator, in which case, accountability would have to be assigned differently.

A study published in 2019 reported the results of a survey where people were asked whether or not an AI could be responsible for its own actions. In situations where a human and an AI were acting together as a team, the human received more of the blame for the result. This is not to say, however, that the human received all of the blame. Remarkably, the results of the study showed that regular people were also willing to put responsibility and blame on the AI as a legal entity.[26]

Naturally, there is a massive difference between the public and the legal community, but lawyers from the NATO Office of Legal Affairs have also raised this question, saying,

> "as noted in a Report from the Global Initiative on Ethics of Autonomous and Intelligence Systems, there was a need to 'address the question of how A/IS should be labeled in the courts' eyes: a product that can be bought and sold? A domesticated animal with more rights than a simple piece of property, but less than a human? A person? Something new?'".[27]

The idea of declaring any sort of legal entity to AI would be upheaval to the legal community worldwide.

This paper does not claim in any way that responsibility for the actions of an AI or AWS should ever be placed solely on the shoulders of the AI. On the contrary, human responsibility should be required whether that be through the operator or through the state that deployed it. The ability to use AI as a scape goat is a large and very real possibility for states to attempt to commit war crimes without repercussions falling on any actual people. Humans must be responsible at least in majority, and securing a legal definition of AI and AWS, while clarifying their classification as an entity or an object, will assist in ensuring such arguments are invalid.

Without a formal legal definition of AI, nor a specific entity to use as a definite example of AI, the result of assigning responsibility to an AI or an AWS is hard to grasp. However, a paper published from the NATO Office of Legal Affairs offers two suggested definitions of AI as "the capability of a computer system to perform tasks that normally require human intelligence, such as visual perception, speech recognition, and decision making," and "technologies that enable machine learning, natural language processing, deduction through vast data-computational power, and ultimately, and automated decision-making in robotics or software that can substitute for tasks once performed exclusively by human action and judgement".[28] If these definitions are to be accepted, then an AWS and a state can be compared to an animal and a human owner. If a dog, left alone outside, were to attack and kill a human, the dog's owner would be held responsible for the dog's actions, but the dog would also likely be put down. Similarly, the state and the specific people who deployed the weapon could be held responsible for AWS committing a crime, but the weapon itself should also be removed from the battlefield and a full investigation conducted.

For most of history, technology that has not functioned as intended did so because it was broken and there was something wrong with it. However, in the case of machine learning and AI, what the system constitutes as correct operation is dependent upon the data it is given and not necessarily the code that it runs. In some cases, AWS can be working perfectly, but still make mistakes. At some level, the AWS is making a judgement and acting on it.

Because AI has yet to have a formal definition accepted by international law, and even more so because AI has not been declared a legal entity, it is hard to establish what accountability would look like for an

AWS. This is a major reason that this paper does not recommend that the possibility of accountability to AWS systems exist now. Instead, it recommends that human accountability be required for AWS, and the in future, when AWS are able to act completely independently, that the AWS also be held accountable for the same actions.

Conclusion

In conclusion, AWS are a vast array of technology that comes in many different forms depending on the "in the loop", "on the loop", or "out of the loop" implementation. Many ideas and theories as to who would be responsible for crimes committed by or using autonomous weapons have been presented, including the idea that programmers, manufacturers, governmental entities that approve their use, or the operators of the weapon itself. As AP I states, a commanding officer is not without responsibility for the actions of their subordinates, and neither is a governmental entity without responsibility for the actions taken by any member of their military.[29] States themselves therefore are responsible for the actions of their military, including AWS. Operators or supervisors likewise would need to be held responsible as they were the humans with the most direct control and dominion over the action of the weapon. Human accountability is, and should always be, required. While DOD policy requires that no off-the-loop, true AWS systems are used in the United States Military,[30] as AI and AWS become more consistent and reliable, it may become the case that true AWS are implemented. In such cases, a formal definition of AI will need to be cemented legally, as well as legal clarification of AI and AWS as an entity or as an object, to ensure that clear legal accountability will not be broken.

The People's Republic of China: Cyber, Emerging Technology, and Grand Strategy

Sean Callis

The United States has experienced many great power struggles in its relatively short history. Because of American innovation, technology has considerably helped the United States preserve its sovereignty. Today, the "Fourth Industrial Revolution"[31] is advancing the world to a new technological plain. Because of the perceived advantages of new emerging technologies, the United States and the People's Republic of China (PRC) have entered a race to develop and use these technologies. Both countries want to apply the advantages offered by these technologies to their respective economies and militaries. Although technology is not the only solution to state superiority, these technologies may help either country gain, or retain, interstate hegemony within the century. China wishes to effectively use these technologies as an enablement factor for their economy and military to dominate their competitors regionally and the United States globally. Specially crafted policies like Military-Civil Fusion are designed to accelerate the development and application of the "Fourth Industrial" technologies to the Chinese economy and military in tandem. In the past 30 years, China has developed a robust cyber operations and espionage program to facilitate the acquisition of important strategic technologies. While the use of revolutionary technology over one's competitors is not unique, the type of technologies being produced today, their pace of development, and the weighted potential that they hold are unique. If the PRC outcompetes the United States through the use of these technologies, the PRC may be able to alter future world systems to their benefit and to the Untied State's detriment. A general introduction to the ideas, context, and Chinese application of emerging technologies to support PRC foreign policy will prove useful to anyone interested in National Security.

What is Chinese Grand Strategy?

> *"The supreme art of war is to subdue the enemy without fighting. Supreme excellence consists of breaking the enemy's resistance without fighting." - Sun Tzu*

China's complex relationship with the United States exists primarily to benefit China and seldom indicates benign long-term interests for the United States. It is important to understand what Chinese grand strategy is, and its general context, according to China's own vision. A primer on this subject will help one appreciate the importance of technology and cyber within Chinese grand strategy. This section will also encapsulate the spirit and reasoning behind China's current policies both within and without the scope of the paper's topic. How technology and cyber are individually applied to the important sectors of economy and military will be explored later in this paper.

According to the Chinese Communist Party's (CCP) "2050 Initiative," Chinese grand strategy goals "are to produce a China that is well governed, socially stable, economically prosperous, technologically advanced, and militarily powerful by 2050." To this end, the "2050 Initiative" hopes to attain "[…] economic growth, regional and global leadership in evolving economic and security architectures, and control over claimed territory."[32] However, key aspects of Chinese state goals collide with the interests of China's regional competitors. U.S. interest-aligned states and territories, such as South Korea, Japan, Taiwan, and the Philippines, have been opposed to Chinese foreign policy. Contention in the South China Sea, competition for engineers in key areas of technological development, territorial sovereignty, and predatory trade practices, are a few examples of contested policy points in the region. Despite opposition, China believes it has the potential to favorably affect these issues and other obstacles through the advantages offered by emerging technologies. However, China's pursuit to become the exclusive regional power over its neighbors is complicated by United States' interests in the region. While China appears to be rapidly climbing to regional and world predominance, China is still not economically, militarily, and technologically equal to the United States. In other words, China cannot compete "blow-for-blow" at this time with the United States and its allies. To compensate, China has devised a strategy to compete asymmetrically with the United States' power advantages and simultaneously pursue Chinese foreign policy goals.

The Competition Continuum

Summarily stated, China envisages the use of all means available, short of open conflict, to achieve dominance over the United States and Her Asian-Pacific allies. To achieve this dominance, China conducts a "sub-threshold of violence" competition against adversaries and competitors. As such, China has expertly placed the pursuit of its national objectives within the competition continuum. The competition continuum extends from "absolute peace" to "total war".[33] Therein ranges several states of competition between countries. These varying states of competition are not definitive but overlap with one another. As competition increases, the "threshold of violence" is met.

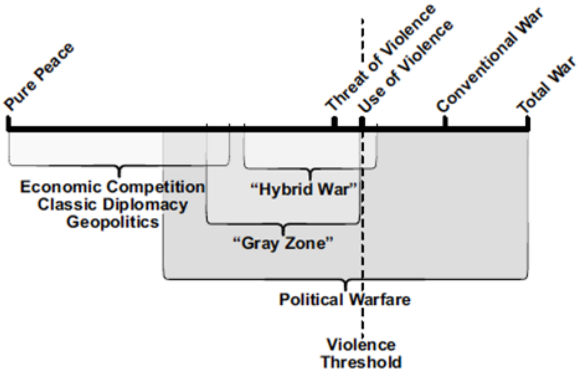

Figure 1. Linear Competition Continuum Model.

This can be defined as military action and the threshold can vary from country to country. China aims to use every possible artifice throughout the continuum to frustrate United States foreign policy while simultaneously achieving Chinese Communist Party (CCP) objectives. Until China sees itself as mature enough to compete in an open hard power struggle, it will attempt to not cross the violence threshold, and rely on soft power (i.e., political warfare) to achieve strategic goals. As defined by George Kenan, "In broadest definition, political warfare is the employment of all means at a nation's command, short of war, to achieve its national objectives."[34] This includes a wide range of resources within the Diplomatic, Information, Military, Economic, Law Enforcement, and Technology DIME(LT) model. The attainment of advanced technologies, and the mastery of cyber operations as foreign policy enablers, are critical to China's asymmetric approach to the United States.

China's trade relationship with the United States is an example of the Chinese prosecution of the "sub-threshold of violence" competition strategy. The United States and the People's Republic of China hold a well-established, symbiotic economic and trade relationship. Much of the new technologies that China needs to develop its economy and military still comes from the United States (e.g., semiconductors, semiconductor producing firm technologies, and supplemental technologies for production). China recognizes the value of the Sino-American trade partnership and leverages it to help themselves monetarily, politically, and technologically. China must carefully manipulate the Sino-American relationship to not hinder their own economic and technological development.

To illustrate further, China's strategic disposition is similar to the United States Army's doctrine of how a light-infantry unit should conduct a raid (a surprise attack similar to an ambush). As conducted, "The assault element [moves] into [an] assault position. The assault position is normally the last covered and concealed position before reaching the objective."[35] Dominance and destruction of the enemy then follows. The PRC's objective is to become the primary influencer of future global systems favorable to their economy and 2050 objectives. Unlike physical topography, like a hill, as the last concealed point before attack, China plans to exploit the Sino-American relationship until the last possible moment. The PRC may then more overtly and aggressively pursue their goals and attempt to nullify the United States at a place and time of their choosing. This is why a sub-threshold of violence-oriented policy, is currently preferred as opposed to increased direct military involvement.

Cyber Warfare

"Avoid what is strong, and strike at what is weak."- Sun Tzu

Cyberwarfare offers a variety of advantages to the PRC. While the reasons mentioned are non-exhaustive, it is helpful to remember why the Chinese state prefers cyber operations. The first, is that the cyber and tech infrastructure of the United States is a soft underbelly. Second, cyber operations are cheap and effective. Third, the context of sub-threshold warfare, cyber can attain large amounts of information from adversaries without their knowledge. Because of cyberwarfare's relative novelty as a strategic tool, there is a lack of clear international law that inhibits the determination of appropriate responses to cyber espionage, infiltration, and attacks, is difficult. Plausible deniability of aggressive cyber operations is an additional advantage to the user. Cyber is the ultimate median through which a conventional and technologically inferior People's Liberation Army (PLA) can level the field against the United States.

Chinese cyber operations dynamically support state goals. This includes three principal areas: "deterrence through infiltration of critical infrastructure; military technological espionage to gain military knowledge; and industrial espionage to gain economic advantage."[36] The contemporary cyber warfare campaign may also be described as two-fold: first, to be used as a deterrence and limit a United States response, and second, to aid in the procurement and development of strategic technologies. The multi-domain campaign to control the United States' response to the PRC's foreign policy is a common theme in PRC strategy. Creating time and space permits China to develop and perfect new technologies in the modern industrial revolution with as little domestic interference as possible. It also provides China the time and space needed to make critical pre-liminary strategic maneuvers to favorably position themselves against their adversaries.

Cyber Operations and Multi-Domain Warfare

Cyberwarfare is an integral part of China's multi-domain system of warfare. Much like any hard power instrument, cyberwar can be used as a deterrent. An HBO Documentary interview covering the North Korean hack of Sony Pictures illustrated the concern that cyberwar gave U.S policy makers. Eric Rosenbach, Pentagon Chief of Staff (2015-2017) lamented, "The last thing you want is to do something that escalates it [the situation] and the North Koreans then hit the United States back in our critical infrastructure. We didn't know whether they were in the grid."[37] Given China's long-term cyber espionage efforts in the United States since the 1990s, it is highly probable that China has extensively mapped many major American domestic systems. The threat of a severe cyberattack can influence when, where, and how the United States will respond. Like North Korea, Chinese infiltration into critical

American infrastructure can be leveraged against the United States. The United States' response to Chinese foreign policy advances may be limited for fear of severe retaliation in this domain. Other areas include the destruction or disruption of the power-grid, sewage and water, communications, banking, and other domestic areas. The disruption of military Information and Communications Technology (ICT) systems can greatly handicap the United States military's decision time and response. It is also possible to purposefully give key policy and decision makers disinformation that can muddle an articulate policy. While all distinct possibilities, continued reconnaissance of United States' systems, protracted manipulation of the American public's views of China, and shaping domestic United States' events through disinformation campaigns, are more beneficial to China at this time than overt policy actions.

Cyber Operations and Technology Acquisition

Cyber operations and espionage help procure the development of key technologies. China, "continue(s) to target a variety of industries and organizations in the United States, including healthcare, financial services, defense industrial base, energy, government facilities, chemical, critical manufacturing (including automotive and aerospace), communications, information technology, or IT, (including managed service providers), international trade, education, video gaming, faith-based organizations, and law firms."[38] These areas of intelligence, technologies, and social influence are the "fuel" for China's cyber/tech-based leg. In the 21st century, China has been technologically inferior to the West. To compete, the attainment of indispensable technologies, both economically and militarily, is crucial for China. The attainment of relevant economic and military information is done by both licit and illicit means, with the latter more prevalent in the realms of Chinese cyber operations. Theft and appropriation of technology is a major contributing factor of China's accelerated growth to their current state of technological advancement. Note, the gathering of intelligence, technological information, and cyber operations, are not mutually exclusive. Newly acquired intelligence and technology can be applied to Chinese cyber operations to increase their effectiveness over time. This compounding effect exponentially increases the value and impact of both cyber operations and acquired emerging technologies. The continued evolution of cyber capabilities gives China a dynamic foreign policy tool to support Chinese grand strategy objectives.

China uses a unique technology and cyber warfare policy to supplement the exploit of the Sino-American relationship. It is in the continued best interest of China to gain large amounts of information and revenue from the United States to fund its strategic ends and technological programs. These programs also conduct espionage of critical technologies from its competitors. The context of cyber discussed is important to keep in mind as it encapsulates the other necessary legs of technologically developing cyber operations, the Chinese economy, and the Chinese military.

How is Cyber and Technology Applied Economically?

"Make the foreign serve China."- Mao Zedong, 1964

A stronger economy equates to a stronger military. A stronger military (and other state resources) allows for an increased ability to enforce one's foreign policy. The creation of a world economic system that is dependent on China, while remaining self-sufficient, is a central objective in contemporary Chinese grand strategy. A technologically independent China will reduce economic disruption and will produce more revenue. While revolutionary technologies double in both economic and military applications, this section will focus on how emerging technologies will aid an independent Chinese economy advance and cement strategic success.

Technology and the Chinese Economy

A technologically robust Chinese economy will produce more revenue. In January 2022, China's State Council released a projected report that, "core industries of the digital economy" will account for 10% of its GDP by 2025, up from 7.8% in 2020."[39] This growth is predicted to continue in the coming decades. To support this development, China has crafted a "Dual-Circulation Economy".[40] The design of a Dual-Circulation Economy is to create a larger domestic consumption of core technology markets at home, while exporting innovative technologies to markets abroad. This may reduce reliance on tech-based products from foreign competitors and outsourcing Chinese consumer's money to foreign markets.

A technologically independent China will reduce outside disruption to the Chinese economy. This was a lesson re-learned after the

COVID-19 pandemic. Although a globally connected world, countries have been re-introduced to the need for some form of economic autonomy and self-reliance. China has established multiple overlapping short, medium, and long-term policies to achieve this. Among these is "Made in China 2025". This plan, "released in 2015, […] is the government's ten year plan to update China's manufacturing base by rapidly developing ten high-tech industries."[41] China plans on achieving seventy percent manufacturing and development independence in these high-tech industries by 2025 and 100% around 2030. While there are ten key technological areas that are being pursued, the "in-house" production of semiconductors, biotechnology, and energy independence will be explored as they are some of the most important.

Strategic Emerging Technology Sectors

Semiconductors are integral components to powering the transformative technologies of the undergoing technology revolution. "Despite their importance, semiconductors represent a rare area in which the Chinese economy is dependent on the rest of the world—rather than the other way around. Every year, China imports more than $300 billion of semiconductors"[42] from multiple countries including the United States and Taiwan. This dependence on its competitors places the Chinese tech economy in a precarious position. As America explores increased trade-independence from China, a geopolitical rift surrounding semiconductors has been created. World trade disruptions after the COVID-19 pandemic have also highlighted the fragility of the semiconductor production/trade-chain. This has spurred a race between the United States and the PRC to become independent semiconductor producers and manufacturers. This would open a massive economic sector for each country and assist in the race for technological supremacy.

Reliable new energy sources are critical for China's strategic goal of an increased independent economy. China seeks to develop "Clean Firm Power" which is, "zero-carbon power that can be relied on whenever it is needed for as long as it is needed"[43] and not solely dependent on when the sun will shine. According to sources attained by Bloomberg, "China accounts for 26% (almost one-quarter) consumption of the world's energy supply. Currently, the majority of Chinese energy production is through fossil fuels by a margin of "31% of global consumption"[44]. The large imports of fossil fuels accounts for China's lack of energy independence. Specialization in the manufacturing and production of alternate energy sources will prove advantageous to China. Employment of vital energy producing technologies would reduce outsourced energy dependence. This change will not entirely eliminate China's need for fossil fuels. Rather, it would diversify the Chinese energy portfolio and introduce what will and will not be worth the effort for future energy production. If China continues to be the primary manufacturer of renewable energy source technologies and components (e.g., solar panels, electric vehicle batteries, wind turbine components, etc.) China can possibly dictate the future of the world energy system. Reliable energy independence will reverse China's position as energy dependent and make other countries dependent on Chinese energy technology expertise. As the West sways towards alternative forms of sustainable energy, and car markets increasingly seek to produce electric vehicles, dependence on China for alternative energy components and technologies may be a reality. Given the rising trend of enmity in the Sino-American competition, this will not be in the American best interest. China may be able to manipulate American response and foreign policy by limiting trade, technology (in multiple areas), and energy resources to the United States, while suffering comparably little due to its future independence in this area.

Biotechnology is another area of exponential economic promise. "As the world's second-largest healthcare market"[45], China seeks to become an innovator instead of exclusively manufacturing biotechnology. There are many pioneering areas within the field of biotechnology to which China can lay claim. Further discoveries in each newly developed area can bring exclusive Chinese rights to the new developments and render vast amounts of revenue. Much like the energy sector, imagine a world here historic breakthroughs in medicine were discovered in China and not the United States. Further imagine what may happen if breakthrough medicinal technologies are not available to Americans because of geopolitical complications between the two countries. These biotechnical and medicinal advantages bring to mind the revolutionary effect that penicillin had for the allied war effort in WWII. While there are a great number of implications that revolve around Chinese biotechnical superiority, it is sufficient to say, that it will be an important sector of competition between China and the West.

How is Cyber and Technology Applied Militarily?

"War is a mere continuation of policy by other means."- Karl Von Clausewitz

Military-Civil Fusion is a keystone PRC policy that lowers the barriers of the private and public sectors. The fusion of private and public sector innovation ensures that both economic and military sectors are developed rapidly in tandem. "MCF is the CCP's strategy to develop the People's Liberation Army (PLA) into a "world class military" by 2049", by way of, "systematically reorganizing the Chinese science and technology enterprise to ensure that new innovations simultaneously advance economic and military development."[46] Chinese national law states that any innovation developed within the private sector must be immediately disclosed and shared with the CCP and PLA. Lowering barriers between private/commercial sectors, the Chinese defense industry, and the CCP, will ensure an expeditious development of both the economy and the military. Artificial intelligence is the main focus of this policy to swiftly develop Intelligentized warfare. Military-Civil Fusion is the master policy that aims to create the world's dominant military with a robust economy to support it.

Intelligentization and Cognitive Warfare

China must outcompete the United States military conventionally and technologically to have strategic success. According to the Association for Science and Technology of the CCP, "technology is not only the foundation and core of advanced military equipment manufacturing, but also the use of advanced technological means is the core of strategic planning, campaign command, tactical application, strategic delivery, and logistical support."[47] The emphasis on emerging technologies has led the People's Liberation Army (PLA) to conceptualize an Intelligentization of warfare. "Intelligentization is the uniquely Chinese concept of applying AI's machine speed and processing power to military planning, operational command, and decision support."[48] This new warfare will leverage "artificial intelligence (AI), quantum, big data, cloud computing the Internet of Things, [and information communication technologies (ICT)], to the military domain."[49] AI is especially sought after because of its key function in cyber warfare and the facilitation of novel System of Systems operations against adversarial militaries. Finally, AI will aid in the expedition of decision-making to create a "cognitive confrontation" with the enemy.

Speed is a decisive factor in warfare. This is why cavalry has been used for centuries and why novel military operations, like the Blitzkrieg, proved so effective. Whoever can receive information, process it, plan, communicate, and execute effectively before the enemy, will have a higher likelihood of victory. Out processing the enemies' OODA loop is the purpose of Intelligentization. Intelligentized warfare also has the previously mentioned "cognitive confrontation" with the enemy's Command and Control (C2) structure and military decision-makers.

> "The essence of cognitive confrontation is knowledge confrontation and intelligence competition [...] which will be used to affect military and civilian morale. Additionally, cognitive measures will be employed to "harass the enemy's command decision-making."[50]

While exact methods are non-specific, the concept of Intelligentization in the cognitive sphere will apply heavily to harassing the enemy Command and Control (C2), operational control, military planning, and population moral and perception. Rapid, preemptive action to the enemy's movements and operational plans diminishes their effectiveness and lessens the enemy's ability to process his own decision-making process. To supplement the "cognitive confrontation", AI can also use misinformation to mislead the enemy. Speed from the marriage of rapid pattern identification and analysis by AI and the human mind may prove pivotal in future warfare.

System of Systems Operations

System of Systems operations are pivotal to the Intelligentization concept. "Chinese military thinkers believe that under the conditions of informatized warfare, dominating a System of Systems confrontation rather than the large-scale attrition of enemy forces is the key factor in winning."[51] In essence, System of Systems operations seek to attack the IT/Informatized basis of the United States military structure. The United States military relies upon extensive Information and Communications Technology (ICT) networks to coordinate joint operations and warfighting. AI, key strategic supporting technologies, and cyber warfare, "is believed to play a central role in Intelligentized warfare to target and crash key elements of opponent operational systems."[52] Within the System of Systems operational doctrine, artificial intelligence will analyze how and where to best conduct crippling attacks on the enemy's command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) structures. If one can cripple or destroy the enemy's C4ISR and ICT structures, while protecting one's own, the odds of victory are exponentially increased.

To illustrate, the entire military operational structure can be compared to the human body. Conventional and kinetic warfare can be equated to a myriad of strikes and parries used by the human body to defeat an opponent. The System of Systems operational dimension opens the possibility of attacking an opponent's "nervous system". The paralyzed, or at best, handicapped opponent becomes uncoordinated. He can then be dispatched, or, preferably, have a higher disposition to surrender the fight (reference cognitive warfare concept in Intelligentization). Instead of solely competing kinetically with the United States, System of Systems warfare is how the PLA may prefer to fight the United States in the future. The PLA desires to be so advanced in this System of Systems field that the United States would prefer not to fight at all. The combination of kinetic, cyber, System of Systems, and cognitive warfare is a holistic approach to attack the PRC's adversaries in multiple dimensions. This will create conditions for more freedom of movement for the CCP to achieve Chinese foreign policy goals.

It is important to note that some form of kinetic action will always be present in warfare.[53] In the PLA's calculus, it is important to not over-extend themselves in kinetic and conventional warfare. This depends on when China feels that it is ready to commit to such a competition, as well as the patience of its leadership to not prematurely do so before the PRC and PLA are ready. Such impatience can bring ruin to China and delay its position to effectively achieve the PRC's foreign policy goals in the future.

Military deterrence is one of the most effective foreign policy tools.[54] It gives force to state policy and can be used as a backstop when alternative options fail to secure state interests. Military deterrence only works when the military is effective enough to "back-up" the state's policies. This is why technology development and integration are so important to the PLA. As cited by Xi Jinping, "Whoever implements scientific and technological innovation well will be able to get a head start and win an advantage." Although the PLA is presently inferior to its American counterpart, the rapid development and application of strategic technologies to the Intelligentization of warfare concept will prove vital to Chinese grand strategy in the coming decades.

Conclusion

Future Chinese grand strategy rests upon leading-edge emerging technologies with the support of cyber operations. The creation of an independent economy through technology will ensure a wealth of resources to develop a world class military. While the pursuit of advancing a country through technology is only one tool in a comprehensive approach, it is not the solution to advancing a country. The technology race is one part of China's advance to hegemony in the century. As seen in many historical instances of great power competition, emerging technology has great potential to be the deciding factor in a competition in parity. The integration of strategic technologies into the Chinese military, if done before the United States, will allow for increased deterrence, and will help secure PRC foreign policy interests. Much like the internet in 1994, little is fully known of the potential poised by technologies like AI, quantum, big data, renewable energy, and biotechnology. What is known, is that if China "turns the curve" before the United States in these sectors, it may be difficult to compete with the People's Republic of China in 2050 and beyond.

China’s Rising Space Program and Its Threat to U.S. National Security

Isaac Garside

Introduction

Over the previous decades, space has helped usher the world into a new age, but it has also become a contended issue among the world’s superpowers. The United States has long been atop the space industry. Way of life throughout the world has forever been altered by technological advancements in space. Cell phones, GPS, and other technologies would not be possible without advancements in space technology. However, many peer competitors are looking to overtake the United States. The biggest of these competitors is China. Along with China’s rise as a near pear competitor to the United States, it has been increasing its research and development of its space technology. China has a very ambitious space program, and it is determined to replace the United States as the dominant space power. Not only are these technologies used for research and development, but for spreading Chinese influence across the world. This poses a major threat to United States global influence and national security.

China’s Tiangong space station, lunar aspirations, and advancing satellite technologies, pose major threats to United States national security. The deterrence of these technologies is paramount to continuing US global supremacy. The United States will need to rely on private industry and academia to further the development of its deterrence technologies.

Tiangong Space Station

To understand the significance of China’s soon to be operational space station, a basic history of the International Space Station is helpful. The International Space Station (ISS) has long been Earth’s lone space station. Having an operational space station has allowed for advancements in many fields of research and development. Being able to conduct experiments as well as monitor conditions on earth and in space has been beneficial to the world. Since the early 2000s, the United States and other countries have continuously had astronauts occupying the ISS. Having the ISS has also led to better diplomatic ties between countries. The legal framework is found in the International Space Station Intergovernmental Agreement, or the IGA. Article 1states that "a long-term international co-operative frame-work on the basis of genuine partnership, for the detailed design, development, operation, and utilization of a permanently inhabited civil Space Station for peaceful purposes, in accordance with international law."[55] In addition, the treaty allowed for Germany, Italy, Japan, Canada, and Russia to work under the United States to accomplish the building and launching of the space station.[56]

China is notably absent from this treaty. During the early 2000s, China was not considered even a regional power. It had not economically developed to where it is today and its absence in space was inconsequential. Space has always been a realm to project power and China not being a part of the ISS has fueled them to create their own space station. Now, China has developed its own space station, the Tiangong, and it will be fully operational soon.

The Tiangong space station has a two-fold purpose. The first is for research and development. Research and development are the foundation of any emerging technology. With space technology, most of the money and resources allocated go to researching and developing better equipment or other projects. As previously stated, there have been several research projects undertaken by the ISS over the years. The second purpose is power projection. Emerging technology is going to be this century's nuclear weapons, meaning that whichever country has the most advanced technology will become the global hegemon. China has long been using its economic influence to project power throughout the world. One example of this is China's Belt and Road initiative where Chinese operated companies build critical infrastructure in developing countries and in turn, China gains more economic influence in the region. Space is another realm China is looking to project its power. With all the technological advancements, space technology is arguably the most used by the average person. China aims to overtake the United

States as the most powerful country in space.

The Tiangong space station aims to replace the ISS as the go-to space station for exploration and research. Over the previous decades, China has slowly developed economic relationships with many countries. These relationships have been one-sided due to the economic influence China has on these countries. To gain more power and influence in space, China needs to continue these relationships. Although China may have the technology to become a leader in space, countries like the United States and Russia have decades of experience in space. China has already publicly partnered with Russia in many of their space programs.[57] If the Tiangong space station is to replace the ISS as the main space station, they will need to internationalize their space station. China will need partners to not only research and develop technology, but the maintenance of the space station.

Although much of the information is not publicly known, there are five major categories that the station will focus on. These are space biology and microgravity physics, fundamental physics, space earth science, space astronomy, and space environment monitoring.[58] Although these do not pose an immediate threat to national security, it is difficult to collect intelligence on research in space. If the United States does not develop more advanced cyber or satellite technology to monitor the research China is doing in space, China can go unchecked at their space station. If they make certain breakthroughs with their technology, it could lead to a major national security threat because the United States would not know the full capabilities of these technologies.

Predicting the full capabilities of China's space program is difficult. Much of their program is classified and the known portions are intentionally left vague. Having an authoritarian government has allowed China to progress very rapidly and judging by this trajectory, their space ambitions can all be accomplished. This has also led to China's rapid growth, both economically and technologically. China can tap into the private industry and academia more quickly than the United States. Research done by these Chinese institutions can be quickly obtained by China's defense department. The United States does not have this advantage. Although heavily reliant on the private industry and academia, the acquisition process of these technologies can take decades to accomplish. This will continue to be an obstacle moving forward but is necessary to advance the United States' space programs.

Lunar Aspirations

Recent reports suggest that after China develops a fully functioning space station, their next ambitions heavily rely on the moon.[59] These include sending probes to the moon and Mars to collect samples and setting up a lunar base to continue their research.[60] A functioning moon base may sound fictious at this time but, when China completes the development of a space station, the development of a lunar base will seem more likely. Currently, China is aiming for a permanent lunar base sometime in the 2030s.[61] Along with the Tiangong Station, the main purposes of this base will be for research and development as well as power projection.

The current plan is for China and Russia to have joint ownership of the lunar base, with the invitation for other countries' involvement.[62] This will be the largest China-Russia cooperative project in space, though not the first. In 1957, the Soviet Union and China signed the New Defense Technical Accord, where Moscow would provide China with nuclear and missile-related capabilities. It was speculated that with the help of Russian assistance, China would be allowed to launch a satellite in 1959 or 1960. However, on arrival in Moscow in 1960, the Soviet Union denied China from viewing their satellite designs or launch sites.[63] In this instance, the Soviet Union hampered China's space program and discouraged them from future space exploration. However, in present day, China holds more power and influence on the international stage and is willing to work with Russia to accomplish this goal. Russia has continuously sided with China on many of these issues and will continue to moving forward.

The major reason for such an ambitious space program is to project power and promote Chinese values across the world. China is quickly becoming a near-peer competitor to the United States and has surpassed it in many fields. Promoting Chinese national pride has a major influence on the space program and if they accomplish these lofty goals, they will in turn project supremacy across the world. Many countries could be forced to side with China if the alternative is not as effective.

There have been many skeptics of the lunar base plans. As of December 2021, there have yet to be any countries to take China and Russia up on their offer to join the lunar research station.[64] Building and maintaining a lunar base will take a substantial number of resources, which China possesses but Russia does not. Russia's space program budget is notably smaller than both China's and the United States'. Becoming equal partners in this endeavor could prove difficult and China could push them out. Without international cooperation, building and maintaining a lunar base is impossible. Also, both countries are on the brink of armed conflict in their subsequent regions. Any form of armed conflict would be detrimental to their space programs and could push back the project for decades.

Historically, the United States has been on the cutting-edge of space technology and research. They have also simultaneously been the global superpower. NASA has been the major organization when dealing with space exploration, space technology, and other technological advancements. NASA also has plans for a lunar base and this conflict could turn into a twenty-first century space race. However, being a U.S. government entity, their resources are limited. The reliance on private industry and academia cannot be understated. Without their help, NASA would be insufficient for the demands of space technology. Private industry and academia needs to have an integral role moving forward for the United States to maintain global hegemony.

Satellite and Anti-Satellite Capabilities

The foundation of a space program is China's ability to develop and launch satellites. Satellites have a wide range of capabilities and the advantage of launching and controlling many cannot be understated. While the United States has launched the most satellites, China has continued to develop and launch satellites at a rapid pace. China has made surveillance of their people a priority, so satellite technology is an important part of its industry. Many of China's satellites have unknown capabilities which poses a major threat for national security. Knowing how China has developed its other technologies, unknown satellite technology could be the most threatening.

One of the satellites that China has developed and launched has the capabilities of capturing enemy satellites.[65] Much like Fortem Technologies DroneHunter program, this satellite is able to target enemy satellites and capture them.[66] We do not know the extent of this satellite's capabilities, but the dangers of China getting ahold of US satellites cannot be overstated. The United States has spent billions of dollars on the production and launch of over one thousand satellites.[67] The protection of our satellites is of utmost importance. The priority is to develop technology to counter this specific satellite. Though the United States is also developing similar technology, China has publicly showcased its abilities and is currently fully functional.

Countering this technology is going to take a great deal of time and resources. We do not yet understand the full extent of China's satellite technology. They have made nondestructive, space based anti-satellite weapons, but we are still unaware of their full capabilities.[68] The priority is to protect our existing satellites as well as guarantee the safety of future projects. The technology that is needed to protect U.S. assets in space can be developed in the private industry. Russia has already shown the ability to destroy satellites in low earth orbit. As previously stated, China and Russia have collaborated on several space projects. Breakthroughs made by both countries can easily be shared between the two and is one of the many threats that the United States' faces in space.

China would not risk a military attack now, but this shows that they have the capabilities to disrupt U.S. satellites. This would be very detrimental to United States' civilian life. If China were to disrupt satellites in charge of navigation and communications, it could black out huge areas of the continental United States. There are also many satellites in orbit with military applications. Not only would the US lose valuable assets, but China would also potentially gain access to US advanced technology.

This is just a few of many examples of China's threat in space. Countering these specific programs will lead to other breakthroughs in space technology. Deterrence is always going to be the goal with any of these emerging space technologies. Developing specific counters is timely and costly but is necessary to ensure security in the United States.

United States Deterrence

As previously stated, deterrence of these technologies is paramount to ensuring national security. Space technology is rapidly advancing and many of the capabilities are unknown. If China were to weaponize some of its satellites or other space technologies, safety would be difficult to achieve. If the public were to be aware of this, it would lead to instability among the population.

The United States' private industry is a major advantage to countering China's space program. Not only is NASA continuing innovation of its technology but the private industry has ambitious goals in space technology innovation. Companies like Northrup Grumman, Lockheed Martin, and Boeing have partnered with DoD and other DARPA programs to advance United States' space capabilities.[69] Although the acquisition of these technologies is not the most efficient, many of the U.S. space advances could not have been possible without private industry.

Although China is launching its own space station, the United States is countering with private industry equivalents. There are three proposed space stations that are being developed by separate companies. Although these companies' stations have different purposes and agendas, they will continue to innovate for the future. This will give the United States a major advantage for space technology.

Conclusion

The United States needs to rely on its private industry more than ever. There are breakthroughs with the research and development of these technologies every day. Academia is also a major partner of private industry in their research. Working with these entities will give the United States an advantage over China and other competitors. Countries with authoritarian systems like China can obtain private industry technology faster than the United States. However, the United States' private industry and academia is more developed. The Tiangong space station is the foundation of China's space program and cannot be understated. China plans on expanding its influence around the world and into space. If the United States wants to remain the global hegemon it needs to counter these advances with its own.

Post-Soviet Lithuania's Quest for Energy Independence from Russia

Michelle Stanley

Introduction

Much of Europe is now striving to reduce their dependence on Russian energy in response to Russia's invasion of Ukraine; however, Lithuania began this process 11 years ago when Russia raised the price of Russian gas transported through Gazprom. The Baltic States – Lithuania, Latvia, and Estonia – have been striving to become independent in this way from Russia since the fall of the Soviet Union. The Baltic States recognized the potential danger of being dependent on Russia and with the Russian invasion of Ukraine, those concerns proved to be well-founded. In May 2022, Lithuania became the first EU country to completely stop using Russian gas.[70]

The main focus of this paper is on the history of Lithuania's energy relationship with Russia from its declared independence from the Soviet Union in March 1990, its complete dependence on Russia for gas, and the process of becoming the first EU country to become independent from Russian gas in May 2022. This is a case study to show that independence from Russian energy removes Russia's coercive power over that country and that the current European energy crisis is the culmination of long-standing European dependence on Russian energy.

This paper begins with Lithuanian historical events that are essential in understanding the topic and is afterward divided into three time periods. First, it examines Lithuania's energy relationship with the Soviet Union/Russia immediately before and after the fall of the Soviet Union. Next, it examines the process whereby Lithuania has pursued its energy independence from Russia since 1991 to the Russian invasion of Ukraine in February 2022. Finally, it examines Lithuania's efforts to achieve full energy independence from Russia following the Russian invasion of Ukraine.

A Brief History of Lithuania

Lithuania is a small country and yet it has a strong cultural and ethnic identity. With a challenging history of protecting its sovereign territory, Lithuanians have had to be wary of relying too heavily on any ally and Russia is no exception. Lithuanians have come to be known for their strength and resilience. This has led Lithuania to have a strong desire to be completely independent from Russia. Although it became politically independent after the fall of the Soviet Union, it has struggled since to establish its energy independence from Russia.

Lithuania's support of Ukraine and rejection of Russia's brutality against Ukraine exemplifies the Baltic States' drive to become fully independent from Russia. Part of Lithuania's foreign policy includes strong motivation to support Ukraine and the necessity to find energy independence from Russia due to the recent invasion of Ukraine. Some have asked why small countries like Lithuania would choose to get involved in support of Ukraine when they are part of the NATO and are therefore safe from militant Russian attacks. One explanation would be that Lithuania chooses to support Ukraine because of the suffering endured by Lithuanians during the Soviet occupation of Lithuania. The Lithuanian people have a poignant view of Russia because of this. In addition, the atrocities and war crimes that were committed against the Lithuanian people happened recently and are still in the minds of many survivors as well as the posterity of survivors.

When post-Soviet countries see Russia acting violently towards a sovereign country it strengthens the government and public's resolve to fight the leader who supports these violent ideals. Just as an attack on human rights somewhere is an attack on human rights everywhere, so an attack on sovereignty somewhere is an attack on sovereignty everywhere. Lithuania used its ability to stop importing Russian gas in 2022 – and help other countries do the same – to show Russia and the world that it is not acceptable to attack an unprovoked, sovereign country.

Lithuania – January 1990

An event that is still commemorated each year on January 13th is an event that illustrates what it was like to live in Lithuania under the occupation of the Soviet and additionally demonstrates Lithuania's dependence on the Soviet Union at the time. This will help to show how much of a transformation Lithuania has made since January 1990. "Laisvės Gynėjų Diena" or Defenders of Freedom Day, began on January 11, 1990, when a group of 250,000 Lithuanian protestors gathered in response to the visit of former Soviet Union leader, Mikhail Gorbachev. With nothing left to lose besides their own lives, the Lithuanian people took to the streets which were full of Soviet soldiers and tanks. These attacks were aimed toward the civilian population.

The protests continued to escalate until tanks surrounded a group of civilians on January 13th when in front of the T.V. Tower in Vilnius, Lithuania, civilians were injured, and fourteen people lost their lives in the cause of freedom. These individuals are honored as martyrs for Lithuania's new-found independence even thirty-two years later. With attacks to suppress the revolution, the Soviet Union fought to control the people and eventually gave way. Lithuania once again reclaimed their own independence on March 11, 1990.

This isolated event cannot fully describe the Soviet occupation in Lithuania; however, it shows the starting point from which Lithuania started in terms of dependence to the Soviet Union. Since Lithuania joined NATO, they have not had to be concerned about Russian military aggression but Russia has continued to assert itself over Lithuania by use of coercive means. These coercive means have been available to Russia through Lithuania's reliance on Russian energy.

Lithuania's Energy Relationship with Russia Following Soviet Union's Collapse

Although Lithuania declared its independence in March of 1990, the Soviet Union did not recognize its independence until the collapse of the Soviet Union at the end of 1991. During the early years of Lithuania's newfound independence, the country struggled significantly economically. Over time, Lithuania regained its footing economically and has gained strength over the years. Although Lithuania was recognized by the Soviet Union as a sovereign country, it still lacked the ability to protect itself from the Soviet Union because of its lack of energy independence.

The years that followed the collapse of the Soviet Union were difficult for Lithuania and every post-Soviet country as they transitioned to become self-reliant again. One of the most significant difficulties of this post-Soviet time was the economic collapse. Lithuania had to rebuild its economy from the ground up after the collapse of the Soviet Union. This was difficult in many ways and led Lithuania to depend heavily on other countries, especially Russia, to get the economy functioning in a somewhat effective way again. This led to the dependence on Russia for energy and specifically gas. This was necessary at the time, in the wake of the collapse of the Soviet Union, due to Lithuania's newfound economic turmoil.

Lithuania's Need for Energy Independence from Russia

In 2012, Russia was supplying all of Lithuania's gas through Gazprom. With this power, Russia was able to increase the price of gas by 30%. Government officials in Lithuania understood that they would have to find a way to use energy from somewhere else to avoid the Russian price increases on 100% of gas imported into Lithuania at the time. Darius Šelenskis, CEO of Lithuanian AB Klaipeda Nafta explained, "Because we are closer, because we are smaller, because we are blackmailed, because we have been occupied for 40 years by the Soviets - so we were always cautious about the suppliers from Russia, and that's why we did homework earlier."[71] By 'homework', Šelenskis meant that Lithuania had to develop an alternative for using Russian gas before the rest of Europe was thinking about becoming energy dependent from Russia. Due to proximity, Lithuania did not have the luxury of waiting until the invasion of Ukraine.

Lithuania's Energy Relationship with Russia Post-Invasion of Ukraine

When Russia invaded Ukraine in February of 2022, Lithuania took a stand against Russia in one of the only ways they were able to - through economic sanctions. Part of the economic sanctions included becoming less reliant on Russian imports and Russian customers buying Lithuanian exports. Due to Lithuania's support of Ukraine and sovereignty, Lithuania has again sought a new independence but this time regarding energy.

When Russia invaded Ukraine in February 2022, Lithuania sanctioned Russia by discontinuing the use of Russian gas along with other exports. In May 2022, Lithuania completely stopped using Russian gas, after a decade of preparation to do so.[72] This preparation was taken in advance, knowing that one day Russia could stop providing gas to Lithuania.

Self-determination is an aspect of state independence and sovereignty. It means a state developing its own government and alliances with other states.[73] Lithuania began to develop itself by embracing self-determination as a country and becoming independent from Russia in providing its own gas. Through this, Lithuania developed alliances and joined organizations such as NATO and the EU. Self-determination is a big part of Lithuania's quest for independence.[74]

The EU is dependent on Russia to provide natural gasses because Russia has plentiful natural resources in terms of natural gas. To hold Russia accountable, several members of the EU have sanctioned Russia by shifting their country's use of Russia energy. Lithuania's Minister of Finance Gintarė Skaistė commented in June that Lithuania's goal is that by the year 2030 Lithuania will use 93% renewable energy sources.[75]

Although Lithuania's economy has taken a significant hit from the Ukrainian war due to the economic sanctions they have placed on Russia, the Lithuanian economy has proven to be resilient.[76] According to the Mena Report, one of the reasons why Lithuania's economy has stayed relatively strong in the face of all this turmoil is because Lithuania has been gradually becoming less reliant on Russia over the last several years since Lithuania joined the EU.[77]

The Significance of Kaliningrad to the Russian Federation

Throughout the years, Kaliningrad has been owned by different sovereign states and was most recently won by Russia. Although the exclave is useful and in a strategic economic location on the Baltic Sea and provides a home for Moscow's Baltic Sea Fleet, Kaliningrad has no bridge to mainland Russia and must rely on Lithuania to transport exports and imports through the country.

In 2022 and after the invasion of Ukraine, Lithuania made the decision to uphold sanctions that were established by the EU to stop EU sanctioned goods from being imported or exported through Lithuania and into Kaliningrad. In addition, Lithuania did not impose any restrictions or sanctions on goods on their own. Russia responded with a comment made by the secretary of the Russian Security Council Nikolai Patrushev that the sanctions Lithuania imposed on Russia were "hostile" and warned that there would be consequences for continuation of these economic sanctions on Russia.[78]

In June 2022, in response to the Russian invasion of Ukraine and in support of Ukraine, Lithuania issued a specific sanction to ban the exportation and importation of specific goods that were sanctioned by the EU from going through Lithuania and into Kaliningrad.

On July 29th, 2022, Lithuania lifted the transport of goods through Lithuania into Kaliningrad according to an article by The Guardian referencing a report made by Russia's RIA news agency.[79] According to the report, this lifting of the ban of transporting goods through Lithuania is likely due to the strong threats Russia gave in response to Lithuania's sanctions.[80]

Because Poland shares its northern border with Kaliningrad, Russia foreign policy significantly affects Poland as well. Recently, Poland has been making its voice heard in rejection of Russia's actions in Kaliningrad and how they are affecting its country. On November 3, Poland made the claim that Putin is "plotting to destabilise Europe with a flood of asylum seekers after Russia's aviation authority approved a raft of new flights from the Middle East and North Africa to Kaliningrad."[81] The worry associated with this action by Russian foreign policy is that the E.U. will not be able to support all the individuals who are seeking asylum. To protect Poland from this plot, Poland made the choice to start building what the Daily Mail London is calling the new iron curtain.[82]

According to the Washington Post, on June 17, 2022, LTG announced that "it would no longer allow Russian goods that are under E.U. sanctions, including coal, metals and construction materials, to transit through the country to Kaliningrad – which the region's governor said would affect nearly half its imports."[83] Subsequently, on June 21, 2022, Russia threatened Lithuania in response to the economic sanctions they began enforcing which stopped allowing E.U. sanctioned Russian goods to be transported through Lithuania to the Russian exclave of Kaliningrad along the Baltic Sea.[84]

Conclusion

By becoming independent from Russia through energy independence, Lithuania has increased its national security and the stability of its economy. The result has exemplified how a small country can gain energy independence from Russia and enjoy the freedom that comes from Russia's inability to blackmail them any longer. In the months that have followed Lithuania's declaration of being energy independent from Russia, many EU countries have followed suit. This has sought to hold Putin accountable for his aggression in Ukraine and will build a Europe that will be prepared to rebuild Ukraine when Russia's invasion in Ukraine concludes.

The Terrorist in Each of Us: An Analysis of the Making of a Terrorist

Kayla Leigh

Almost everyone's life has been impacted by terrorism in some way, whether by having to go through T.S.A. at the airport or going through metal detectors at a sports game. Since 9/11, the incidents of terrorism have continued to increase globally at an alarming rate. Along with the growing threat of terrorism, the way that everyday life has been affected by terrorism, both domestically and abroad, continues to grow. Before the 20th century, many countries didn't experience terrorists as an everyday problem, but the reality now is that every country must be ready and aware of any threat made by a violent extremist. A recent study done by Irena González and her research team, titled "Evidence of Psychological Manipulation in the Process of Violent Radicalization: An Investigation of the 17-A Cell," looked in depth at a 17-A terrorist cell in Spain that has been known to commit violent attacks. Their research is aimed at understanding psychological manipulation and how it led everyday individuals towards committing violent acts. The team found that in 2019, 119 attacks and over 1,000 incidents relating to terrorism occurred and from those attacks, "approximately 70% were between 20 and 28 years old, and roughly 60% ... were citizens of the country where the attack took place".[85] It is no longer just foreign actors that are committing deadly terrorist attacks, but rather citizens are now turning to terrorism. Understanding why this process continues and finding a way to prevent terrorism is vital to stopping deadly attacks from occurring.

How does an individual who has had no signs of violent extremism or mistrust in their government turn to such violent extremism? Some argue that terrorism is bred by individuals who have suffered from mental health issues. Although this was a respected and popular theory in the 90s, recent studies show that it is inaccurate. One recent study done by Margot Trimbur et al, "Are Radicalization and Terrorism Associated with Psychiatric Disorders? A Systematic Review," looked at the psychological profiles of 2,856 known terrorists and known extremists to try to see if claims of underlying mental health issues were present. At the conclusion of their systematic review, they stated, "We were not able to identify a significant association between radicalization, terrorism, and psychiatric disorders in our systematic review".[86] This old theory is no longer relevant. Rather, society must look at other factors that create terrorists rather than believing terrorists are extremists from birth. Randy Borum is a professor at the University of South Florida who teaches coordinated strategy and intelligence studies. Borum is also a licensed psychologist. He has published papers on national security, threat assessments, violent extremist information science, and the psychology behind terrorism. In his article, "Psychology of Terrorism," Bourm looks at many outside factors that push people towards terrorism. He argues that contrary to what many psychologists believed in the '90s, "Mental illness is not a critical factor in explaining terrorist behavior. Also, most terrorists are not 'psychopaths.'... There is no 'terrorist personality,' nor is there any accurate profile – psychological or otherwise – of the terrorist".[87] Rather, Borum argues it is the outside factors that create individuals who would consider terrorism a viable option in their lives. In this paper, I intend to argue that violent extremists or terrorists are created through a system of radicalization that targets those with economic struggles and works through psychological manipulation and socialization. It is through these areas that radicalization occurs, and terrorists are created.

Economic decline, as well as social stress, builds a pathway that pushes individuals toward terrorism. There are many economic and social environments that create individuals who feel as if they aren't being heard by the governments that are charged with improving the lives of their citizens. Many countries that experience economic hardship have seen a rise in terrorism that correlates with the economic downturn. In a study done about this correlation by Seung-Whan Choi and Shali Luo, who both received PhDs from the University of Missouri focusing on international economics, wrote a study titled "Economic Sanctions, Poverty, and International Terrorism: An Empirical Analysis" where they analyzed the impact of poverty and economic sanctions on the growth of terrorism. In their study, they looked at countries with low economic opportunity and how that affected the rise of terrorism. They cited a report showing that "countries with higher levels of economic inequality are associated with higher levels of terrorism".[88] With less economic opportunity to grow, people get frustrated in the environment they are in. When individuals are unable to provide for their families and loved ones, they look to someone to help them change things. If their government won't help, then they will look for someone who will. This oftentimes leads people toward groups that, in perfect circumstances, they wouldn't consider. Borum highlights a model developed by Frederick Hacker that explains this process in several stages;

> "The first stage involved an awareness of oppression. The second stage marked a recognition that the oppression was 'social' and therefore not unavoidable. The third stage was an impetus or realization that it was possible to act against oppression. Ultimately, at the end point of that phase, some conclude that working through advocates intermediaries (e.g., elected officials) or within the system to 'reform' or improve it is not going to work and that self-help by violence is the only effective means for change".[89]

Oftentimes, mistrust in your government develops through the feeling of not being heard or taken care of. When economic turmoil leads to mistrust in the government, people will look for someone to blame for their problems.

There are many times when a person has been wronged and will turn to others to blame. These perceived injustices can be a major factor in violence and aggression. Borum writes that "Perceived injustice has long been recognized as a central factor in understanding violence generally and terrorism specifically, dating back to some of the earliest writings".[90] The idea that you have been wronged unjustly by a group of people can make anyone feel angry. But if you combine that idea with the fact that you are being wronged by the people who are supposed to have your best interests in mind, it can create a sense of hopelessness that can be dangerous. It doesn't matter if the person in question has actually been slighted but rather if the individual believes they have been slighted. This will produce the same amount of anger and aggression as if the person has actually been wronged. Borum points out "The process begins by framing some unsatisfying event or condition as being unjust. The injustice is blamed on a target policy, person, or nation. The responsible party, perceived as a threat, is then vilified – often demonized – which facilitates justification for aggression".[91] One's perceived reality is more important when it comes to getting involved with terrorism than the actual reality of the slight. If a person feels like they are at a disadvantage to their government, when in reality they aren't, they will still act in a way that reflects that belief of injustice.

A sense of injustice helps create a group ideology centered and based on this "injustice." The group will now base its actions and recruiting on finding ways to get back at those who have placed this injustice upon it. In an article written by Michael Arena and Bruce Arrigo, professors of criminal justice at the University of North Carolina at Charlotte wrote a paper titled "Social Psychology, Terrorism, and Identity: A Preliminary Re-examination of Theory, Culture, Self and Society." Arena and Arrigo examine past theories of terrorism and reflect on what they believe are the true causes of terrorism rather than the past belief that mental illness is the sole driving factor of terrorism. In their findings, they discuss the theory of perceived injustices. The authors review a report finding that when an individual feels that they are being neglected or kicked out of their society they turn to violence and anger.[92]

This idea contributes to an individual's sense of abandonment by the people who are supposed to protect him. It helps create this narrative that you are being robbed of something that is rightly yours. In this state of mind, you are in the right to act out to ratify this. You often see this train of thought in many terrorist organizations. Such as the known terrorist group, The Proud Boys, which is a neo-fascist, anti-women, white nationalist group. In their frame of mind, they feel as if the "Aryan race" is being attacked by the public. They see it as their job to protect the race from further harm and attack. The perceived injustice to them makes it so, in their eyes, they are doing not only the right thing but what god intended. Despite the reality that they aren't being attacked, they still think they are at war. This creates unstable people who will do dangerous things. These perceived injustices and truths push people to act in a manner that normally they would not consider and creates violent extremism.

Through perceived injustices and economic turmoil, terrorist cells are able to use an environment where individuals are vulnerable to being manipulated into radicalized terrorists. Finding normal citizens and radicalizing them into violent extremism happens through a system of psychological manipulation that has several steps. González et al. explain that "The evidence suggests that terrorist groups use psychological manipulation techniques…by creating psychological submission… making the individual feel identified, understood, and valued".[93] Targeting individuals who would be good candidates is something that might differ in groups, but the underlying manipulation tactics stay the same. Groups tend to target individuals that don't have many connections and are isolated. The use of psychological manipulation is often done in ways that are small and go unnoticed by the person these groups are trying to manipulate. The goal of psychological manipulation is to change the way of thinking of individuals to meet the mindset of the person manipulating them. When manipulation like this occurs, the person being manipulated has no idea that this is occurring. "Some scientific studies have compared terrorist dynamics with those applied in cults, highlighting certain similarities between the two…[the] only difference being the use of fear and violence by terrorist groups as a means of self-assertion".[94]

One of the most important parts of turning a recruit into a member of a terrorist organization is radicalization. "I use the familiar term *radicalization* to refer to the process of developing extremist ideologies and beliefs, and the term *action pathways* (or action scripts) to describe the process of being involved in terrorism or engaging in violent extremist actions".[95] The process of turning an individual to extremism through psychological manipulation can occur almost anywhere. Recruiters have been known to come in contact with individuals at schools, churches, clubhouses, bars, etc. Once the relationship has been established, the manipulation slowly begins.

There are three categories of psychological manipulation and radicalization that González and her team found which are common in terrorist recruitment. The first category is cognitive control. Cognitive control is a term used in psychology that refers to the deliberate and intentional selection of emotions, behaviors, and thoughts presented to an individual to try to control habits and behaviors. Over 50% of psychological techniques found by González and her team were considered cognitive control.[96] This is done by controlling the information that a recruit has access to. This can be done by limiting internet access and access to the outside world. Another way this is done is by giving recruits propaganda and information that have been doctored to align with the ideals and "truths" the group believes. At this stage, there are many lies that are told based on beliefs the individual already has such as religion. An example of this technique is the use of the Quran in many Islamic terrorist groups. They will take something that an individual already believes in, such as the Quran, and twist the words to support their violence and claims. This method is considered doctrinal radicalization.[97] This process creates a system where the personal views of the individual being recruited now reflect the view of the group. Another tactic is creating a belief in the leader of the group as well as in the group mentality. Establishing a leader that you should respect and believe in completely creates a system of dependence on the leader and the group as a whole.

Doctrine radicalization contributes to the next two forms of manipulation which are environmental control and emotional control or emotional radicalization.[98] "Among these techniques, we find emotional activation of joy, activation of fear, guilt, and anxiety, as well as rewards and punishments".[99] The goal of this manipulation is to separate the recruit from their current life both physically and emotionally. The group will want the person they are recruiting to be completely dependent on them. They will try to distance the recruit from anyone or anything important in their life using lies and deceptions. The group wants to be able to control every aspect of the recruits' life, and that can't happen if they are around others not in the group. This form of emotional manipulation is often done by encouraging the recruited individual to spend time with the group as a whole. Slowly that attendance with the group will become more important than attending other events. The emotional happiness of the recruit will be dependent on the group as a whole. Eventually, the dependence on the group becomes one's whole life and social circle. An individual won't have any connections outside of this circle. All recruits know and the people with whom they have contact will be controlled by this group. This control will slowly add to the breakdown of the individual's free thinking and opinions to the point that a person will eventually believe what the group believes.

> "Finally, in the third phase of violent disinhibition and legitimization (violent radicalization), the recruit validates the

> use of violence by associating it with the mistreatment and oppression allegedly suffered by their new group, identifies the enemy, and shifts responsibility by making an attack essential to improving their situation".[100]

Once the violent act has been made, the recruit is now tied to the group forever. The recruit is now a full member of the cell and no longer has any ties in the world that aren't connected to this organization. There is no way out of this group.

As discussed previously, along with psychological manipulation, social relationship and self-images play a role in why people join terrorist cells, as well as why they stay in them. "In radical extremist groups, many prospective terrorists find not only a sense of meaning but also a sense of belonging, connectedness, and affiliation" in these groups.[101] Through psychological manipulation, individuals who are being recruited will other times have a sense of self in these groups. They are able to create their own self-image after that of the group, cementing the fact that they are part of the group. Being part of a group, recruits oftentimes find a sense of meaning and belonging that they did not have in their lives before. This occurs when "the leader managed to merge members' 'personal self' with the 'group self,' which promoted a feeling of belongingness that compensated for the conflict of identity and restored the meaning of individuality".[102] Recruiters will often target individuals with a low sense of self due to the fact that they will be drawn to the comfort that can be found in a group setting and environment.[103] A person with a low self-image will feel as if they have found belonging and a family as well as a purpose in life within this group. Due to this feeling of acceptance, the group will become especially important to the person being recruited. The group will make individuals feel as if they have found what they have been looking for their whole lives. It creates a false sense of reality within the group. It also allows for the perceived injustices to now apply to the new recruit.

Due to the fact that the group as a whole finds something unacceptable, the recruit will find it unacceptable to create a new core belief. The recruit will also find committing violent acts acceptable due to the fact that it is done in the name of the group and that the rest of the group has done it as well. The importance of the relationship with the group as a whole should not be understated when it comes to terrorism. It is the group relationship that not only attracts people to terrorist organizations but also keeps people within the network.

Terrorism is a global issue that will affect everyone if something is not done to help prevent radicalization and recruitment. As technology has increased, the ability for organizations to recruit young people all over the world is more accessible than ever. The rise of single-cell organizations that are radicalized over the internet continues to affect and endanger people everywhere. It doesn't matter what nationality you are; terrorism doesn't leave anyone out. Being able to understand what leads people to not only sympathize with violent extremists but to believe as they do is very important. Understanding what goes into radicalization and the tactics that are used are critical so we can stop them once we identify what's happening. There is no gene that makes one a terrorist. Everyone has the potential to become a terrorist, so it is essential to see the signs that a person is being radicalized. It may be the only way to stop the continued rise of terrorism before it becomes too late.

Endnotes

[1] Department of Defense, “Directive 3000.09,” Directive 3000.09 § (201 7), Glossary, Part II Definitions.

[2] Id.

[3] Id.

[4] Id.

[5] Stephen Hill and Nadia Marsan, “ARTIFICIAL INTELLIGENCE AND ACCOUNTABILITY: A MULTINATIONAL LEGAL PERSPECTIVE,” NATO Science & Technology Organization, July 18, 2018, https://www.sto.nato.int/, page 6.

[6] Department of Defense, “Directive 3000.09,” Directive 3000.09 § (201 7), Glossary, (4)(a).

[7] Department of Defense, “Directive 3000.09,” Directive 3000.09 § (201 7), Glossary, (4)(a)(1).

[8] Department of Defense, “Directive 3000.09,” Directive 3000.09 § (201 7), Glossary, (4)(a)(2).

[9] International Committee of the Red Cross, “Autonomous Weapons: The ICRC Remains Confident That States Will Adopt New Rules,” International Committee of the Red Cross, May 30, 2022, https://www.icrc.org/en/document/icrc-autonomous-adopt-new-rules, paragraph 3.

[10] International Committee of the Red Cross, “Autonomous Weapons: The ICRC Remains Confident That States Will Adopt New Rules,” International Committee of the Red Cross, May 30, 2022, https://www.icrc.org/en/document/icrc-autonomous-adopt-new-rules, paragraph 4.

[11] International Committee of the Red Cross, “Autonomous Weapons: The ICRC Remains Confident That States Will Adopt New Rules,” International Committee of the Red Cross, May 30, 2022, https://www.icrc.org/en/document/icrc-autonomous-adopt-new-rules, paragraph 16.

[12] International Committee of the Red Cross, “Autonomous Weapons: The ICRC Remains Confident That States Will Adopt New Rules,” International Committee of the Red Cross, May 30, 2022, https://www.icrc.org/en/document/icrc-autonomous-adopt-new-rules, paragraph 5.

[13] “PROTOCOL ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, AND RELATING TO THE PROTECTION OF VICTIMS OF INTERNATIONAL ARMED CONFLICTS,” accessed December 4, 2022, https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf, Article 36.

14 "PROTOCOL ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, AND RELATING TO THE PROTECTION OF VICTIMS OF INTERNATIONAL ARMED CONFLICTS," accessed December 4, 2022, https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf, Article 85 (3)(a).

15 "PROTOCOL ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, AND RELATING TO THE PROTECTION OF VICTIMS OF INTERNATIONAL ARMED CONFLICTS," accessed December 4, 2022, https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf, Article 85 (3)(a).

16 "PROTOCOL ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, AND RELATING TO THE PROTECTION OF VICTIMS OF INTERNATIONAL ARMED CONFLICTS," accessed December 4, 2022, https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf, Article 86.

17 "PROTOCOL ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, AND RELATING TO THE PROTECTION OF VICTIMS OF INTERNATIONAL ARMED CONFLICTS," accessed December 4, 2022, https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf, Article 87 (1).

18 "PROTOCOL ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, AND RELATING TO THE PROTECTION OF VICTIMS OF INTERNATIONAL ARMED CONFLICTS," accessed December 4, 2022, https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf, Article 91.

19 Stephen Hill and Nadia Marsan, "ARTIFICIAL INTELLIGENCE AND ACCOUNTABILITY: A MULTINATIONAL LEGAL PERSPECTIVE," NATO Science & Technology Organization, July 18, 2018, https://www.sto.nato.int/, page 7.

20 NATO, "Summary of the NATO Artificial Intelligence Strategy," NATO, October 22, 2021, https://www.nato.int/cps/en/natohq/official_texts_187617.htm, page 2.

21 U.S. Department of Defense, "U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway," Department of Defense, June 2022, https://media.defense.gov/2022/Jun/22/2003022604/-1/-1/0/Department-of-Defense-Responsible-Artificial-Intelligence-Strategy-and-Implementation-Pathway.PDF.

22 International Committee of the Red Cross, "ICRC Position on Autonomous Weapon Systems," International Committee of the Red Cross, February 26, 2022, https://www.icrc.org/en/document/icrc-position-autonomous-

weapon-systems, page 2.

23 “Problems with Autonomous Weapons,” Stop Killer Robots, accessed December 4, 2022, https://www.stopkillerrobots.org/stop-killer-robots/facts-about-autonomous-weapons/.

24 International Committee of the Red Cross, “ICRC Position on Autonomous Weapon Systems,” International Committee of the Red Cross, February 26, 2022, https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems, page 2.

25 NATO, “Summary of the NATO Artificial Intelligence Strategy,” NATO, October 22, 2021, https://www.nato.int/cps/en/natohq/official_texts_187617.htm, page 2.

26 Shank, Daniel B., et al. “When Are AI versus Human Agents Faulted for Wrongdoing? Moral Attributions after Individual and Joint Decisions.” 5, May 2019, pp. 648–663.

27 Stephen Hill and Nadia Marsan, “ARTIFICIAL INTELLIGENCE AND ACCOUNTABILITY: A MULTINATIONAL LEGAL PERSPECTIVE,” NATO Science & Technology Organization, July 18, 2018, https://www.sto.nato.int/, page 7.

28 Stephen Hill and Nadia Marsan, “ARTIFICIAL INTELLIGENCE AND ACCOUNTABILITY: A MULTINATIONAL LEGAL PERSPECTIVE,” NATO Science & Technology Organization, July 18, 2018, https://www.sto.nato.int/, page 3.

29 “PROTOCOL ADDITIONAL TO THE GENEVA CONVENTIO_NS OF 12 AUGUST 1949, AND RELATING TO THE PROTECTION OF VICTIMS OF INTERNATIONAL ARMED CONFLICTS,” accessed December 4, 2022, https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf, Article 87.

30 Department of Defense, “Directive 3000.09,” Directive 3000.09 § (2017).

31 Doshi, Rush. “The United States, China, and the Contest for the Fourth Industrial Revolution.” Brookings. Brookings, March 9, 2022. https://www.brookings.edu/testimonies/the-united-states-china-and-the-contest-for-the-fourth-industrial-revolution/.

32 Scobell, Andrew, Edmund J. Burke, Cortez A. III Cooper, Sale Lilly, Chad J. R. Ohlandt, Eric Warner, and J.D. Williams. “China’s Grand Strategy.” RAND Corporation, July 24, 2020. https://www.rand.org/pubs/research_reports/RR2798.html.

33 MCDP 1-4 Competing." U.S Marine Corps - Department of the Navy, n.d. https://www.marines.mil/Portals/1/Publications/MCDP%201-4.pdf?ver=fGwjmqkxGvv0GPe0mPgdqw%3d%3d.m Includes Graphic on The Continuum of Competition

34 Kenan, George. The Inauguration of Organized Political Warfare, April 30, 1948.

35 Essay. In Ranger Handbook: Not for the Weak or Fainthearted. Washington, D.C.: Headquarters, Department of the Army, 2017, 5-14 bullet F.

36 Hjortdal, Magnus. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," July 1, 2011. http://www.jstor.org/stable/10.2307/26463924?refreqid=search-gateway.

37 The Perfect Weapon. United States: HBO, 2020. https://www.hbo.com/movies/the-perfect-weapon.

38 "China Cyber Threat Overview and Advisories." CISA. Accessed April 11, 2022. https://www.cisa.gov/uscert/china.

39 Kharpal, Arjun. "From 6g to Big Data, China Is Looking to Boost Tech's Share of Its Economy." CNBC. CNBC, January 18, 2022. https://www.cnbc.com/2022/01/18/china-looks-to-boost-techs-share-of-gdp-by-2025-through-6g-big-data.html#:~:text=In%20a%20document%20released%20last,runs%20from%202021%20to%202025.

40 "Will the Dual Circulation Strategy Enable China to Compete in a Post-Pandemic World?" ChinaPower Project, March 17, 2022. https://chinapower.csis.org/china-covid-dual-circulation-economic-strategy/.

41 "Is 'Made in China 2025' a Threat to Global Trade?" Council on Foreign Relations. Council on Foreign Relations. Accessed April 11, 2022. https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade.

42 Thomas, Christopher A. "Lagging but Motivated: The State of China's Semiconductor Industry." Brookings. Brookings, January 8, 2021. https://www.brookings.edu/techstream/lagging-but-motivated-the-state-of-chinas-semiconductor-industry/.

43 "California Needs Clean Firm Power, and so Does the Rest of the World Three Detailed ..." Accessed April 11, 2022. https://www.edf.org/sites/default/files/documents/SB100%20clean%20firm%20power%20report%20plus%20SI.pdf.

44 "How China Plans to Win the Future of Energy." Bloomberg.com. Bloomberg. Accessed April 11, 2022. https://www.bloomberg.com/news/

articles/2022-03-15/how-china-plans-to-win-the-future-of-renewable-energy.

45 “China - Healthcare.” International Trade Administration | Trade.gov. Accessed April 11, 2022. https://www.trade.gov/country-commercial-guides/china-healthcare#:~:text=As%20the%20world’s%20second,sales%20sector%20for%20foreign%20businesses.

46 “The Chinese Communist Party’s Military-Civil Fusion Policy - United States Department of State.” U.S. Department of State. U.S. Department of State, December 1, 2020. https://2017-2021.state.gov/military-civil-fusion/index.html.

47 “ [Accelerate the construction of military-civilian integration innovation system].” Accessed April 11, 2022. http://www.qstheory.cn/dukan/qs/2017-08/03/c_1121422420.htm.

48 User. “199. ‘Intelligentization’ and a Chinese Vision of Future War.” Mad Scientist Laboratory, December 18, 2019. https://madsciblog.tradoc.army.mil/199-intelligentization-and-a-chinese-vision-of-future-war/.

49 Jing, Yuan-Chou. “How Does China Aim to Use AI in Warfare?” – The Diplomat. for The Diplomat, January 3, 2022. https://thediplomat.com/2021/12/how-does-china-aim-to-use-ai-in-warfare/#:~:text=AI%20is%20believed%20to%20play,the%20form%20of%20intelligentized%20warfare.

50 “A Chinese Concept of ‘Cognitive Confrontation’ in Future Warfare.” Accessed January 27, 2023. https://community.apan.org/cfs-file/__key/docpreview-s/00-00-22-83-67/2021_2D00_09_2D00_01-A-Chinese-Concept-of-_1C20_Cognitive-Confrontation_1D20_-In-Future-Warfare-_2800_Hurst_2900_.pdf.

51 “China - Healthcare.” International Trade Administration | Trade.gov. Accessed April 11, 2022. https://www.trade.gov/country-commercial-guides/china-healthcare#:~:text=As%20the%20world’s%20second,sales%20sector%20for%20foreign%20businesses.

52 Id.

53 Bilal, Arsalan. “Hybrid Warfare – New Threats, Complexity, and ‘Trust’ as the Antidote.” NATO Review. Nato Review, November 30, 2021. https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

54 “Strong Deterrence Enables U.S. to Ensure Global Rules, Rights.” U.S. Department of Defense. Accessed March 15, 2023. https://www.defense.gov/News/News-Stories/Article/Article/3235400/strong-deterrence-enables-us-to-ensure-global-rules-rights/.

55 International Space Station Intergovernmental Agreement. Article I. January 29, 1998.

56 Id.

57 Andrew E. Kramer and Steven Lee Myers. Russia, Once a Space Superpower, Turns to China for Missions. The New York Times. September 16, 2021

58 Gu Yidong et al. Science Researches of Chinese Manned Space Flight. Technology and Engineering Center for Space Utilization, Chinese Academy of Sciences. July 27, 2014.

59 Kaelan Deese. Chinese official unveils future moon mission plans including possible lunar base. THE HILL. December 17, 2020.

60 Id.

61 Andrew Jones. China Aims for a Permanent Moon Base in the 2030s. IEEE Spectrum. September 22, 2021.

62 Andrew Jones. China, Russia Open Moon Base Project to International Partners, Early Details Emerge. SpaceNews.com. April 26, 2021.

63 Nathaniel Rome. A Chinese-Russian Moon Base? Not So Fast. Foreign Policy.com. October 17, 2021.

64 Id.

65 Mandy Mayfield. "China's Ambitious Space Programs Raise Red Flags." National Defense Magazine, July 2, 2021. https://www.nationaldefensemagazine.org/articles/2021/7/2/chinas-ambitious-space-programs-raise-red-flags

66 Fortem Technologies. "Fortem DroneHunter Successfully Defeats Drone Threats in US Army Test." AP News, September 23, 2021. https://apnews.com/article/technology-business-2eff3e64aa33dc15827dc011fe44bd0d

67 Therese Wood. "Who owns our orbit: Just how many satellites are there in space?" World Economic Forum. October 23, 2020. https://www.weforum.org/agenda/2020/10/visualizing-easrth-satellites-sapce-spacex

68 Mandy Mayfield. "China's Ambitious Space Programs Raise Red Flags." National Defense Magazine, July 2, 2021. https://www.nationaldefensemagazine.org/articles/2021/7/2/chinas-ambitious-space-programs-raise-red-flags

69 Admin. Top 3 Biggest Private Space Companies. Earth.com. https://www.earth.com/earthpedia-articles/top-3-biggest-private-space-companies/

[70] "Lithuania has become the 1st European country to stop using Russian gas." All Things Considered, May 26, 2022, NA. Gale In Context: Global Issues (accessed April 15, 2023).

[71] Id.

[72] Id.

[73] Mccorquodale, Robert. 2021. "The USSR and Its Influence on Developments in the Right to Self-Determination." Brown Journal of World Affairs 28 (1): 1–9.

[74] Id.

[75] "Lithuania: Minister of Finance: 'Green Transformation - European Guarantor of Energy Independence and Resilient Economies'." Mena Report, June 14, 2022, NA. Gale In Context: Global Issues (accessed November 8, 2022).

[76] "Lithuania: Against the background of global shocks, the Lithuanian economy is showing resilience." Mena Report, June 14, 2022, NA. Gale In Context: Global Issues (accessed November 8, 2022).

[77] Id.

[78] "Lithuania: The Lithuanian and Polish Presidents discussed regional security and support for Ukraine." Mena Report, 25 Oct. 2022, p. NA. Gale General OneFile, Accessed 8 Nov. 2022.

[79] "Russia-Ukraine war: what we know on day 150 of the invasion; Lithuania lifts rail ban on goods transport to Kaliningrad; three bodies recovered from Kramatorsk school attack Russia-Ukraine war: see all our coverage." Gua rdian [London, England], August 2, 2022, NA. Gale OneFile: News (accessed November 8, 2022).

[80] Id.

[81] Daily Mail (London, England). 2022. "Poles Start Building a New Iron Curtain; 130-Mile Razor- Wire Barrier to Seal Border amid Fears of Kremlin Plot to Flood EU with Asylum Seekers," November 3.

[82] Id.

[83] Francis, Ellen, and Rachel Pannett. "Russia threatens Lithuania for enforcing E.U. sanctions on Kaliningrad." Washington Post, June 21, 2022, NA. Gale In Context: College (accessed November 8, 2022).

[84] Id.

[85] González, Irena, et al. "Evidence of Psychological Manipulation in the

Process of Violent Radicalization: An Investigation of the 17-A Cell." Frontiers in Psychiatry, vol. 13, Feb. 2022. EBSCOhost, https://doi-org.ezproxy.uvu.edu/10.3389/fpsyt.2022.789051.

86 Trimbur, Margot, et al. "Are radicalization and terrorism associated with psychiatric disorders? A systematic review." Journal of Psychiatric Research, Vol. 141, 05 July 2021, pp.

214-222, DOI: 10.1016/j.jpsychires.2021.07.002.

87 Borum, Randy, "Psychology of Terrorism" Mental Health Law & Policy Faculty Publication", 2004, 22-69, https://www.ojp.gov/pdffiles1/nij/grants/208552.pdf.

88 Choi, Seung-Whan, and Shali Luo. "Economic Sanctions, Poverty, and International Terrorism: An Empirical Analysis." International Interactions, vol. 39, Apr. 2013, pp. 217–45. EBSCOhost, https://doi-org.ezproxy.uvu.edu/10.1080/03050629.2013.7684

89 Borum, Randy, "Psychology of Terrorism" Mental Health Law & Policy Faculty Publication", 2004, 22-69, https://www.ojp.gov/pdffiles1/nij/grants/208552.pdf.

90 Id.

91 Id.

92 Arena, Michael, and Bruce Arrigo, "Social Psychology, Terrorism, and Identity: A preliminary Re-examination of Theory, Culture, Self and Society" Behavioral Science and the Law, Vol. 23, January 2005, pp. 485-505, https://discovery-ebsco-com.ezproxy.uvu.edu/c/y34kcw/viewer/pdf/36aunqsmgj.

93 González, Irena, et al. "Evidence of Psychological Manipulation in the Process of Violent Radicalization: An Investigation of the 17-A Cell." Frontiers in Psychiatry, vol. 13, Feb. 2022. EBSCOhost, https://doi-org.ezproxy.uvu.edu/10.3389/fpsyt.2022.789051.

94 Id.

95 Borum, Randy "Rethinking Radicalization." Journal of Strategic Security, vol. 4, Jan. 2011, pp. 1–6. EBSCOhost, discovery.ebsco.com/linkprocessor/plink?id=4c43bc2b-2bd9-3fe4-b2d9-182a291c743f.

96 González, Irena, et al. "Evidence of Psychological Manipulation in the Process of Violent Radicalization: An Investigation of the 17-A Cell." Frontiers in Psychiatry, vol. 13, Feb. 2022. EBSCOhost, https://doi-org.ezproxy.uvu.edu/10.3389/fpsyt.2022.789051.

[97] Id.

[98] Id.

[99] Id.

[100] Id.

[101] Borum, Randy, “Psychology of Terrorism” Mental Health Law & Policy Faculty Publication”, 2004, 22-69, https://www.ojp.gov/pdffiles1/nij/grants/208552.pdf.

[102] González, Irena, et al. “Evidence of Psychological Manipulation in the Process of Violent Radicalization: An Investigation of the 17-A Cell.” Frontiers in Psychiatry, vol. 13, Feb. 2022. EBSCOhost, https://doi-org.ezproxy.uvu.edu/10.3389/fpsyt.2022.789051.

[103] Arena, Michael, and Bruce Arrigo, “Social Psychology, Terrorism, and Identity: A preliminary Re-examination of Theory, Culture, Self and Society” Behavioral Science and the Law, Vol. 23, January 2005, pp. 485-505, https://discovery-ebsco-com.ezproxy.uvu.edu/c/y34kcw/viewer/pdf/36aunqsmgj.