Cyber Shadows II:

Navigating Space Cyber Warfare at the National and International level

By: Jackson Murphy

1. Introduction:

In today's era of interconnectedness, our dependence on technology is deeply ingrained into the very functioning of society. From communication and finance to healthcare and transportation, the seamless functioning of technology sustains every aspect of our lives. However, this reliance introduces vulnerabilities, especially in the cyber and space-cyber domains. The digital battleground, where state-sponsored actors wield cyber weapons, is expanding to include space-based assets, making satellite systems a critical point of concern. The advent of the internet and rapid technological advances have revolutionized society and introduced cyber conflict, fundamentally altering international relations and warfare. As technology evolves exponentially and conflict increasingly incorporates digital means, laws governing technology—specifically its malicious use against nations' space-based assets—have struggled to keep pace. In exploring the shadowy world of space-cyber warfare, this paper seeks to illuminate the existing landscape, compare it to traditional kinetic conflicts, and address the challenges of establishing international norms and laws. Only through comprehensive global governance can we hope to maintain peace and security in the digital era while navigating the unique challenges of space-cyber warfare. In doing so, this paper aims to provide insights into the lacking current state of national and international cyber law and propose pathways, if not create discourse at the very least, for effective governance, abroad and at home, which is critical for maintaining international peace and security in the digital era.

2. Approach:

In subsection 3.1 of the “Survey of Existing Techniques/Solutions,” a historical context and technical understanding of space systems, including satellites and their

components, are introduced to provide readers with a foundation for the subsequent discussion. In subsection 3.2, cyber and space-cyber weapons and attacks are analyzed and compared with traditional cyber weapons. Subsection 3.3 explores the historical intersection between space and cyber warfare, presenting a brief history of the space-cyber-war nexus both nationally and internationally. This context sets the stage for understanding current and future legal and ethical challenges. In subsection 3.4, the intricacies of international law concerning cyber warfare and space are discussed. In subsection 3.5, the application and challenges of international law for space cybersecurity are elaborated. Section 4 synthesizes this information into practical suggestions for improving national and international legal frameworks. Finally, section 5 concludes by emphasizing the need for a renewed commitment to international collaboration and legal frameworks capable of keeping pace with evolving digital threats in space.

3. Survey of existing techniques/solutions

3.1 Introduction to Satellites

Background

The first satellite “Sputnik 1” was launched into orbit on October 4th, 1957, by the Soviet Union.[1] The United States, who had already been developing its own satellite, launched Explorer 1, the first U.S. satellite just a few months later, on January 31, 1958.[2] Since then, space (and cyber) technology has exponentially grown. Space systems in the modern era are highly complex vehicles, costing anywhere from hundreds of thousands of dollars to all the way upwards of tens

[1] NASA. "Sputnik and the Dawn of the Space Age."
[2] Tepper et al.

or even hundreds of millions. For instance, commercial satellites such as BlueBird cost between $16-$18 million[3] each, and a US military contract for a satellite constellation (made up of 18 satellites) was awarded valued at $515 million.[4] The expense lies in the process of designing, developing, and launching satellites into the earth's orbit. Not only do they have to withstand an immense amount of force put on them for the rocket to be able to reach escape velocity but satellites “operate in extreme temperatures from −150 °C (−238 °F) to 150 °C (300 °F) and may be subject to radiation in space”[5] while in orbit.

Components

For space systems there are generally three main components that work together as one unit. These three components include the space segment, the ground segment and the link segment.

Space Segment

The space segment is the only part of a satellite system in which people traditionally think of. When people think of a satellite, often it is a singular entity but the space segment “includes all spacecraft involved in the satellite operations, which may be just a single satellite or an entire constellation. These satellites are initially launched into orbit using a launch vehicle, i.e., a rocket, and then undergo an orbital deployment phase to initiate communications with the ground segment.”[6]

Ground Segment

The ground segment, also known as the earth or terrestrial station, is the point on earth in which the space segment interacts with. This segment is crucial for communicating with and operating the space segment once it has been deployed into space. “The ground segment is the center of all satellite operations throughout the entire lifetime of a satellite. A team of operators

---

[3] Henry
[4] Erwin
[5] Encyclopedia Britannica
[6] Fritz, Maus, et al.

communicates with the satellite using a Ground Station (GS) to provide new instructions to the satellite, referred to as Telecommand (TC). In turn, the satellite sends Telemetry (TM) back to the GS, providing information about the satellite's status, errors, and other metrics."

Link Segment + Communication Protocols

The link segment is composed of two separate parts, the uplink and the downlink. This is also known as TT&C. "The TT&C uses radio-frequency (RF) links between the space element and the ground. As the name suggests, it performs three fundamental tasks: Command (also known as telecommand, TC), Telemetry (TM), and Tracking" and with this "A satellite's TC/TM traffic is communicated via a satellite communications protocol"[7] Satellites (space segment) communicate to and from the ground (ground segment) over a wide range of radio frequencies which often include UHF, S, X, and Ka for small satellites and Ku, K, and Ka for larger satellites as well as inter-satellite connections.[8] The communication protocols are one of the most targeted aspects by malicious actors as signal encryption is minimal or non-existent.

Uses + Orbits

The orbit of a spacecraft is generally dictated by what a satellite is being used for. The three primary types of orbits include Low Earth Orbit (LEO), Medium Earth Orbit (MEO), and Geosynchronous Earth Orbit (GEO). For purposes of discussion, the primary focus will be on satellites in LEO as they account for 55% of operational satellites and 90% of all satellites in space.[9] They are also largely used by governments in their security and communication capabilities. Regardless, the following applies to all satellites, not just those in LEO.

A Brief History of the Space-Cyber-War Nexus, Nationally and Internationally

1941 - Development of Z3, the first programmable computer[10]
1957 - Soviets launch Sputnik 1. First satellite successfully launched into space. [11]

---

[7] Modenini and Ripani, "A Tutorial on the Tracking, Telemetry, and Command"
[8] NASA, "Small Satellite Institute"
[9] CSIS, "Earth Orbit 101"
[10] Computer History Museum, "Timeline"
[11] NASA, "Sputnik History"

1958 - US launches Explorer 1[12]
1967 - Outer Space Treaty[13]
1972 - ARPANET was introduced, precursor to the internet[14]
1985 - US Space Command is established[15]
1991 - The first gulf war is seen as the "first space war" as dubbed by Air Force General Merrill McPeak. Notably it is seen as the root for the militarization of space and highlighted the need for space-based capabilities within a military campaign.[16]
1995 - Creation of the Information Warfare squadron.[17]
1998 - Researchers become aware of 'Moonlight Maze', the first example of an ATP. Its purpose was purely for intelligence gathering, much like Duqu.[18]
2001 - Budapest Convention on Cybercrime[19]
2007 - Russia launches cyber attack against Estonia targeting financial services and media with DoS attack. First well known example of a state being targeted in a cyberattack.[20] The first version of Stuxnet was released under the bush administration.[21]
2010 - Discovery of Stuxnet, the first cyber weapon that had physical implications, which affected Iranian US enacts Title 51 on National and Commercial Space Programs.[22]
2016 - NATO declare cyberspace a new operational domain[23]
2019 - US Space force is established[24]
2020 - US national space policy makes space a warfighting domain[25] SPD-5 enacted by the Trump administration.[26] First comprehensive policy on the cybersecurity of space systems.
2022 - Viasat attack. First cyber attack on a satellite used for a military objective.

3.2 Defining Space Cyber Weapons and Attacks

Difficult to define

It is difficult not only for the US government to define what a cyber weapon is, but the international community as a whole, yet it is nevertheless necessary. In order to understand the issues of internationally regulating cyber weapons and attacks we must first actually define what

[12] NASA, "Explorer 1 Overview"
[13] UNOOSA, "Outer Space Treaty"
[14] The Conversation, "How the Internet Was Born"
[15] Gazette, "History of Space Command in Colorado Springs"
[16] Tepper et al.
[17] Kumite, "609 IWS"
[18] ScienceDirect, "Moonlight Maze"
[19] Council of Europe, "The Budapest Convention"
[20] Council on Foreign Relations, "Estonian Denial of Service Incident"
[21] Stanford, "Stuxnet"
[22] U.S. Government, "Cybersecurity Policy Recommendations"
[23] RAND Corporation, "RAND's Perspective on Space Security"
[24] U.S. Space Force, "History"
[25] Federal Register, "The National Space Policy"
[26] Trump White House Archives, "SPD-5"

they are in order to understand them. International law has long been restricting and regulating certain weapons dating back thousands of years. For example “The Dharmasutra of Baudhayana (ca. 500-200 BC) contained similar restrictions on violence…This code also “contained a restriction on permissible weapons that the belligerents can wield against one another; it prohibited the use of barbed or poisoned weapons”[27] Even more recently anything from chemical weapons under the Geneva Protocol in 1925 to the more recent Non-Proliferation Treaty in 1970 which discouraged the use of nuclear weapons, international bodies have sought to regulate weapons throughout history, both past and present. While this is the case for many kinetic weapons, reputable sources are lacking for virtual. Our society continues to be ever more so digitally connected. With the very functioning of our society resting upon the functioning of the internet, we still have no clear precedent to look to from any reputable international governing body about cyber weapons. And the problem still remains: How can an international body regulate something that they struggle to a consensus on? To understand cyber attacks and conflicts (especially those that are state sponsored) it may be beneficial for us to first actually define what cyber weapons are. In order to do this, it might help to first look at real weapons and draw comparisons with cyber weapons.

Real weapons vs cyber: Real weapons

What are weapons? Weapons are used to manipulate and/or control an entity in order to further a specific goal at the expense of the victim. A soldier might shoot their enemy to further their military objective, a cop might shoot a perpetrator to stop them from committing further violence or an assassin might take out a governmental leader to stage a coup. Oxford public international law defines weapons as “a thing designed, intended or used for inflicting bodily harm or physical damage; a means of gaining an advantage or defending oneself”[28]. To elaborate on this definition, notice the use of intention. A weapon is not necessarily a weapon until it is used in

[27] Neff, p. 17.
[28] “Weapons, Prohibited”, OPIL

the manner a weapon would be used. A knife isn't a weapon, it is a tool, but when used to attack someone it then becomes a weapon. Further weapons can also be used for the threat of harm as much as the actual harm itself. For instance, a thief might use a knife to threaten someone in order to steal their belongings without actually stabbing them, thus a threat that causes a desired outcome at the expense of someone else via said tool can be seen as an attack/weapon. Next both weapons and attacks need credibility that a threat is able to be carried out. Going back to our example of the thief using a knife, now imagine that this knife is actually made of plastic. As long as the victim believes the knife to be real then it is still a weapon. Now on the other hand the victim notices the knife to be instead made of plastic, it is no longer a weapon[29]. Thus, the credibility for a threat to be undertaken is a necessity. A single person holding a knife likely isn't going to be able to take down a government, but a thousand or a hundred thousand people very well might be able to. Lastly for a weapon to actually have been used there needs to be some sort of impact because of the weapons use, and the impact of this weapon or attack will have varying levels of severity based on the implications of the use. Going back to the knife example, someone threatening to use a knife to steal a purse is less severe than someone using the knife and stabbing someone to get the purse, which is less severe than thousands of people using knives to overthrow a government.

Definition: Real weapon

A thing that is meant to create harm by either the action itself or the credibility of using the thing in order to achieve a goal at the expense of the victim, which is judged in severity based on the implications of the aforementioned use.

Use: How was the weapon used to control or manipulate an entity
Purpose: Why was the weapon used, what was the benefit to the attacker
Aspects: What were the attackers' intentions, are they able to follow through with them
Impact: What are the direct & indirect consequences of said use of weapon to the victim(s)

[29] (adapted from Cyber-Weapons, McBurney, Rid)

Cyber Weapons

So how do we then apply this definition of weapons towards the cyber sphere? Let's break down cyber weapons with our previous definition of a weapon.

Use: To control or manipulate an entity, either digitally OR physically, via code
Purpose: To utilize a cyber weapon in a way that benefits the attacker
Aspects: The attackers intentions, and are they able to follow through with them
Impact: Direct & indirect consequences of said use of weapon to the victim(s), with the consequences solely digital or are they physical as well

Definition: cyber weapon

Thomas Rid & Peter McBurney put it perfectly that cyber weapons are simply weaponized software/code or "computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings." We can expand on this with the previous definition of weapons and say that cyber weapons are - "A code or software that is meant to create harm, either digitally or physically, by either the action itself or the credibility of using the thing in order to achieve a goal at the expense of the victim, which is judged in severity based on the implications of the aforementioned use, (and it's severity is equivalent to that of something in the real world)."

Traditional vs. Space: Space Cyber Weapons

Traditional Cyber Weapons

To recap, cyber weapons consist of malicious code or software designed to manipulate digital systems. They aim to control or harm entities through digital means, affecting systems or data that ultimately can influence real-world functions.

Space Cyber Weapons

Just as traditional cyber weapons manipulate systems, space cyber weapons aim to affect entities in the space domain. However, their targets are primarily space assets, which have unique vulnerabilities due to their physical and technical characteristics.

Use: To control or manipulate the space-based ecosystem, such as satellites or ground stations, via cyber means. They could be used to disrupt communication links, manipulate sensor data, or interfere with control systems.
Purpose: To exploit space systems for strategic gains, like disrupting communications, impacting navigation systems, or causing orbital debris by manipulating space assets. Attackers may aim to gather intelligence, degrade infrastructure, or inflict financial and reputational damage.
Aspects: Attackers' intentions to carry out attacks on space infrastructure and their ability to achieve those objectives. This could involve advanced persistent threats and complex, multi-stage attacks that exploit both space and ground-based systems.
Impact: The consequences of such attacks could be significant, as they can affect not just the space infrastructure but also terrestrial services reliant on satellite technology. Disrupted GPS, communication blackouts, and disabled military satellites could all have far-reaching effects.

Definition: Space Cyber Weapons

Space cyber weapons are a specialized category of cyber weapons designed to affect the space domain. They involve software or code aimed at compromising space systems, with intentions ranging from espionage to sabotaging critical infrastructure. The implications are broader due to the interconnectedness of space systems with terrestrial networks and the potential for cascading failures.

Space cyber weapons are malicious code or software designed to target space infrastructure, with the intent to threaten or cause physical, functional, or informational damage to space assets, their ground systems, or the services they provide.

Cyber Attacks (generally)

Rule 92 of the Tallinn Manual claims that a cyber attack is characterized by its ability to inflict harm or damage through cyber means, regardless of whether the harm is physical or not, and irrespective of the direct target being a cyber system or data.[30] Space cyber weapons are the tools/means used to implement the more general cyber attack[31]. As with real and cyber

[30] Part IV.17 Section 2, Tallinn Manual

[31] ***Why the emphasis on cyber weapons?*** As for later discussions of international cyber law, cyber attacks will be the primary focus and cyber weapons the secondary. This is due to how international law is often used (which is touched on later). Let's take the example of a more traditional warfare setting— while some weapons are regulated such as the previously mentioned nuclear weapons, their regulation more so deals with the entities that are committing the attacks using said weapons. Going back to our example of traditional warfare, less emphasis is placed on the guns of soldiers themselves and more so on what those soldiers are

weapons relatively having similar uses the same can be said about cyber attacks and their conventional counterparts. The means of any weapon is to exert nonconsensual control over another entity, cyber attacks have the power to do this across borders utilizing cyber weapons.

Cyber Attacks, in Space

While discussed more in depth in the subsequent section on international law, according to Rule 112 in The McGill Manual on International Law Applicable to Military Uses of Outer Space, "Cyber activities that constitute space activities, including military space activities, are governed by international space law, as well as the applicable rules of general international law."[32] So generally speaking and in terms of international law, any basis from which cyber activities (such as weapons and attacks) are being discussed, the same can be said about space cyber activities.

Weapons & attacks vs non-weapons & attacks

One of the struggles with trying to define cyber weapons and attacks is that not all things that might fit under some part of our definition fully meet the criteria for said definition. A great example of this would be the comparison between the two viruses, Stuxnet and Duqu.

Case Study #1: Stuxnet vs. Duqu

Stuxnet

Not all cyber attacks are clear cut uses of cyber weapons. This is not the case for the Stuxnet virus. Stuxnet is a definite example as it took computer code and weaponized it in a way that had real world implications or as discussed in *Stuxnet: the emergence of a new cyber weapon*

---

doing with said guns and their authorization to use said guns. The purpose of detailing cyber weapons in such great extent is to ground the reader due to the novel nature of cyber weapons and to highlight the comparison between kinetic and cyber which will be incessantly discussed. Further, while the emphasis of studying warfare is largely the study of the entities committing the acts of war, it is still important to understand the features of the weapons. i.e. as of recently the study of drone warfare has become a big topic of discourse, with the emphasis being placed on the weapon itself. However, with both nuclear weapons and drones, one cannot understand their uses and ethical implications of their use without understanding first the weapons themselves.

[32] Jakhu and Freeland

and its implications, "unlike the malware that came before it, is highly targeted and designed to achieve a real-world outcome". The Stuxnet virus was likely[33] created during the Bush and into the Obama administration as it was believed that Iran was on the verge of developing atomic weapons. Israel proposed an airstrike against the nuclear facilities, but this had the threat to set off a regional war so Operation Olympic Games[34] was seen as the nonviolent alternative. The virus was used to attack Iran's nuclear centrifuge in Natanz. More specifically, Stuxnet was a highly sophisticated piece of malware that exploited zero-day vulnerabilities on Windows operating systems, specifically targeting Siemens industrial control systems. Through reprogramming of these ICSs, Stuxnet was able to cause physical damages. This virus was said to be "the most sophisticated cyberweapon ever deployed against another country's infrastructure."[35] and further "Kaspersky Lab's Roel Schouwenberg estimated that it took a team of ten coders two to three years to create the worm in its final form."[36] Further because of "the size and sophistication of the worm have led experts to believe that it could have been created only with the sponsorship of a nation-state"[37]. The significance of Stuxnet was that while once thought to only have the ability to attack the digital realm, the Stuxnet virus highlighted to the general public the possibility that weaponized computer code could not only affect digital services, but it also has real world implications, especially in international conflict, as well.

It follows our definition of a cyber weapon as:

Use: It was used to manipulate an enemy (Iran) via code (Stuxnet)
Purpose: Stuxnet was used because of the fear of Iran possessing nuclear arms and to derail the Iranian program to develop nuclear weapons
Aspects: A real act that did take place
Impact: destroyed Iranian centrifuges while it also set back their nuclear program at least 2 years

---

[33] No one ever claimed responsibility but its code signature was similar to that of US & Israeli agencies
[34] Code for Stuxnet virus
[35] Valeriano, Maness, "Persistent Enemies and Cyberwar," 102.
[36] O'Gorman, "Stuxnet Explained"
[37] Kushner, "The Real Story of Stuxnet"

Duqu

Unlike the previously mentioned Stuxnet, which is a prime example of the weaponization of computer code as it had physical consequences, Duqu (and Duqu 2.0) does not follow our definition of a cyber weapon or attack as closely. Duqu malware was first discovered in 2011 and was said to have similar coding style to Stuxnet, so much so that it is believed that they were written by the same authors.[38] Duqu is also similar to Stuxnet not only in style of code used but it being one of the most "Sophisticated malwares encountered in the recent past"[39] and more importantly that it was likely state sponsored as "The Duqu 2.0 operation displays no objective of getting any financial profit from the use of the Malware. The use of multiple zero-day exploits and sophisticated hacking techniques during the attack is another indicator that it is a nation-state sponsored campaign."[40] meaning it also was used to further the goals of a nation-state. While similarities remain, aside from the aforementioned aspects, Duqu can be seen diverging from Stuxnet. Duqu, unlike Stuxnet, was not meant to cause any physical harm and instead was used for cyber espionage and to collect intelligence. According to Rule 32 of the Tallinn Manual, "The International Group of Experts agreed that customary international law does not prohibit espionage *per se*."[41] For the time being understand that international law does not generally find cyber espionage to be illegal, unlike the case of Stuxnet which broke a number of international laws, infringing on state sovereignty, intervention, use of force… among other things. Using our own definition of cyber weapons, Duqu also does not qualify as one as. A cyber weapon is:

"computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings."

---

[38] Valeriano, Maness, "Persistent Enemies and Cyberwar,"
[39] "Managing trust in cyberspace" p. 403
[40] Kaspersky, "Duqu 2.0: Frequently Asked Questions."
[41] Part I.5, Tallinn Manual

Which we broke this down as:

Use: To control or manipulate an entity, either digitally OR physically, via code
Purpose: To utilize a cyber weapon in a way that benefits the attacker
Aspects: The attackers intentions, and are they able to follow through with them
Impact: Direct & indirect consequences of said use of weapon to the victim(s), with the consequences solely digital or are they physical as well

With Duqu the primary problem is the use and impact. As with the definition of a cyber weapon, there was no 'aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings', and with our broken-down version, Duqu was not used to control or manipulate an entity and the consequences were not substantial enough for it to be warranted as a weapon.

Case Study #2: ViaSat and AcidRain

ViaSat - *The First Space Cyber Attack*

What makes the attack on ViaSat so noteworthy in space cybersecurity is that it can be seen as the first space cyber attack used to further a military objective. ViaSat, a satellite communication company was attacked by Russia on February 24th, 2022, just an hour before the invasion of Ukraine, impacting their KA-SAT network. Specifically two pieces of the ground segment were attacked, "the modems of individual users and the modem control servers."[42] The point of entry for attackers was "localized to a single consumer-oriented partition of the KA-SAT network that is operated on ViaSat's behalf by a Eutelsat subsidiary, Skylogic"[43] At 03:02 UTC, high volumes of malicious traffic were detected coming from modems in Ukraine, and while ViaSat as well as Skylogic personnel worked to remedy the situation, more modems continued to go offline. At 04:15 UTC, ViaSat and Skylogic noticed vast amounts of modems crashing throughout Europe

[42] ResearchGate
[43] ViaSat

for another 45 minutes.[44] Thousands of modems went offline over the KA-SAT network, and remained inoperable for days to months. What allowed this attack to happen was "a poorly configured VPN appliance" where the attacker then was able to "access to the segment of the network used to manage and operate it, and then pushed legitimate, yet malicious, commands to residential modems in Ukraine and several other European countries."[45] More specifically ViaSat notes, " The attacker moved laterally through this trusted management network to a specific network segment used to manage and operate the network, and then used this network access to execute legitimate, targeted management commands on a large number of residential modems simultaneously."[4647]

AcidRain - *The First Space Cyber Weapon*

AcidRain can be seen as the weapon that was used to deploy the ViaSat attacks. As a spokesperson from ViaSat further noted when talking about the attack, "Specifically, these destructive commands overwrote key data in flash memory on the modems, rendering the modems unable to access the network"[48] On March 15, researchers at SentinelOne discovered AcidRain, the malware used to attack the system, after it was uploaded to VirusTotal from a user in Italy.[49] The goal of this malware is to "brute-force device file names and wipe every file it can find, making it easy to redeploy in future attacks."[50] Generally, the goal of the attack was to destabilize and disrupt the Ukrainian army's communication as well as further hinder their defenses, but this attack affected entities outside of the conflict such as customers in Europe, or

[44] ViaSat
[45] The Register
[46] ViaSat
[47] Murphy, "Space Cyber Post Mortem"
[48] ViaSat
[49] TechCrunch
[50] BleepingComputer

even “5,800 German wind turbines”[51][52] Further on its purpose, the malware includes using IOCTLs[53] to erase file content and it performs a deep wipe of the filesystem and device files, rendering devices inoperable by targeting modems, routers, and IoT devices. AcidRain bears similarities to past Russian-linked malware, particularly VPNFilter, which also targeted networking equipment. Although they differ in some ways, both utilize the MEMGETINFO, MEMUNLOCK, and MEMERASE IOCTLs to wipe data and share some code similarities, suggesting possible shared origins or techniques. One independent researcher found that they were 55% similar, thus likely being Russian.[54] “The US has concluded Russia’s own military intelligence service, known as the GRU, orchestrated the cyber attack on ViaSat”[55], all other Five Eyes agencies have concluded the same, but Russia has refuted the claim, a problem discussed in the latter section on challenges. At this point there is a working definition of a cyber weapon, and for this case study we simply are applying it to space. Much like Stuxnet and Duqu, the same methodology can now be applied to AcidRain.

Use: AcidRain was used to manipulate targeted network infrastructure, primarily Viasat's KA-SAT network, through malicious code that systematically erased key device files.
Purpose: The primary goal of the AcidRain malware was to destabilize and disrupt Ukraine’s military communication infrastructure by wiping modems and other connected devices, leaving them inoperable and effectively undermining Ukrainian defenses.
Aspects: The attackers intended to exploit vulnerabilities within the KA-SAT network to access modems and push destructive commands. By erasing critical data and disrupting the communication network, they aimed to degrade Ukraine's military response capabilities, which they successfully achieved.
Impact: The AcidRain attack directly impacted the KA-SAT network, leading to the mass outage of thousands of modems across Ukraine and Europe, thus hindering communication capabilities. This attack had ripple effects beyond Ukraine, disrupting commercial services and highlighting the potential for cyber weapons to cause widespread digital and physical consequences, making it an unequivocal demonstration of cyber warfare.

---

[51] MIT Technology Review
[52] Murphy, “Space Cyber Post Mortem”
[53] Input/Output control system calls
[54] SentinelOne, "AcidRain: A Modem Wiper Rains Down on Europe"
[55] PCMag, "Report: US Concludes Russia’s Military Was Allegedly Behind ViaSat Hack"

Takeaway: AcidRain, like Stuxnet, illustrates the growing capacity for cyber attacks to have tangible effects in the physical world, setting a precedent for the use of malware as a weapon in international conflicts and against space assets.

3.3 National and International Law

National Context

Generally

Most people, citizens of the US at least, are much more familiar with national law than they are international. Regardless, a brief refresher will be given for those who are familiar with it, or a brief crash course for those who are not. In terms of national law, nationally it is much easier to understand and interpret law as there is codified law which the government looks to. For the most part, there are four main sources of law in the American legal system: the Constitution, federal statutes, regulations, and case law.

The constitution

The U.S. Constitution is the nation's fundamental law. It codifies the core values of the people. Courts have the responsibility to interpret the Constitution's meaning, as well as the meaning of any laws passed by Congress. For the most part this does not apply to the space-cybersecurity nexus, but is seen as the supreme law of the land.

Federal Statutes

Federal statutes are laws that are enacted by Congress and signed by the president. They provide specific legal frameworks that federal agencies and courts follow. Statutes can also be codified into the United States Code, a compilation that organizes federal law by subject matter for ease of reference. Relevant examples might include; the communications Satellite Act of 1962, which provided a framework for international satellite communications[56] or the

[56] US Government, "Communications Satellite Act of 1962"

Cybersecurity and Infrastructure Security Agency Act of 2018 which established CISA to safeguard critical infrastructure.

Regulations

Federal regulations are rules created by federal agencies to implement and enforce laws passed by Congress. These regulations have the force of law and guide how the agencies administer various programs. Relevant regulations might include NIST's (National Institute of Standards and Technology) Cybersecurity Framework which guides federal agencies and private companies on cybersecurity best practices including those relevant to space-related infrastructure.

Case Law

Case law, also known as judicial precedent, consists of decisions made by federal courts, including the Supreme Court, appellate courts, and district courts. These decisions interpret the Constitution, federal statutes, and regulations, providing binding precedent for future cases. There is very little precedent for space cybersecurity in the US but one example might include United States v. Drummond (2006) which involved satellite signal piracy and addressed the illegal interception of satellite communications.

Laws: Cybersecurity + Space?

For the following two bills, they have been proposed in the Senate and House, but have not been passed into law at the time of this writing. Both are waiting on approval from their respective committees and need full approval, not just partial. The third is not a bill, like either of these, so it has gone into effect

Space cybersecurity act

The Satellite Cybersecurity Act (S.3511) aims to enhance the cybersecurity of space-based systems, primarily focusing on satellites and their supporting infrastructure. The bill emphasizes the assessment and management of cybersecurity risks, the development of standards and best practices, and the promotion of collaboration between public and private sectors to improve

incident response. It also supports research for innovative solutions to emerging threats and establishes reporting requirements for cybersecurity incidents to strengthen threat intelligence. Overall, the act seeks to safeguard satellite infrastructure by improving cybersecurity practices and fostering cooperation across sectors.[57]

Space infrastructure act

The Space Infrastructure Act (H.R.5017) aims to classify space infrastructure as critical, thereby ensuring prioritized protection and support. It encourages investment by providing federal funding and incentives to boost public and private space initiatives. The legislation also emphasizes collaboration between government and private entities to drive innovation, strengthen partnerships, and enhance the U.S. space industry's global competitiveness.[58]

***Space Policy Directive-5,* Non-binding**

Space Policy Directive-5 also known as SPD-5 was released in September of 2020 and is the first policy of its kind combining the areas of space and cybersecurity. SPD-5 establishes principles to guide the cybersecurity of space systems. It emphasizes enhancing the resilience of space assets by promoting the adoption of cybersecurity best practices across the industry. The directive encourages public-private collaboration to secure space systems, fosters innovation in cybersecurity solutions, and prioritizes risk management to protect against emerging threats. SPD-5 sets a foundation for enhancing the cybersecurity of space systems to safeguard national and economic security.[59] The large challenge with SPD-5 is that it is “non-binding and treated mostly as informational”[60], so while a step in the right direction, there is still a large gap between this and what needs to be further implemented in the US.

[57] Senate, "Satellite Cybersecurity Act"
[58] House, "Satellite Cybersecurity Improvement Act of 2023"
[59] Trump White House, "Memorandum on Space Policy Directive-5"
[60] Plotnek and Slay

Recap

For the most part while US law is easier to work with than the subsequent international law, it is still very much lacking for space cybersecurity. Because space assets operate in a much more global context than a national one, the remainder of the discussion will focus on international law.

International Context

Popularity - Weapons

Cyber weapons in general have grown increasingly popular in recent years as tools for nation-states to exert control in the international landscape compared to traditional kinetic means. New means of warfare are cheaper than traditional means, they are harder to attribute to a specific government (and thus plausibly deniable), they can be highly targeted and reach across the globe in mere seconds, the threshold of engagement is lower, and they can disrupt without physical destruction needing to take place. According to a research brief compiled by Foreign Policy Analytics, “Cyberspace is now a strategic domain as states use cyber tactics to conduct stealth attacks on rivals and target private industry for espionage and commercial gain, helping to level the geopolitical playing field.”[61] Further it can be seen that cyberattacks continue to gain popularity among state actors as “from 2017 to 2020 the frequency of state-sponsored cyberattacks doubled, with an average of 10 publicly attributed cyberattacks per month in 2020. Threat actors’ techniques have also advanced, making them harder to identify and more threatening to targets.”[62] and “Out of 94 cases of cyberattacks reported as financial crimes since 2007, the attackers behind 23 of them were believed to be state-sponsored”[63] As these cyber attacks continue to increase in both popularity with state actors, and the volume of attacks

[61] Foreign Policy Analytics, "The Rise of State-Sponsored Cyber Attacks and the Cost of Inaction,"
[62] Foreign Policy Analytics, "The Rise of State-Sponsored Cyber Attacks and the Cost of Inaction,"
[63] Reuter, “Cyber Attacks on US Banks”

taking place, it is a necessity to continue to understand and create legal framework surrounding them.

Popularity - Space Cyber weapons

Much that can be said about the general 'cyber weapon' can also be said about space cyber weapons, taking this one step further. As previously mentioned, developing and launching space assets is a costly endeavor. This is an important factor as the expense/impact ratio is much higher for malicious cyber attackers. On the ground, singular technological assets of such a high value are much more heavily guarded against cyberattacks than their space based counterparts. Space assets, as briefly mentioned, are very vulnerable to cyber attacks, and this combined with their evermoreso necessary use by the military make cyberweapons prime modes of attack for nations looking to create a large scale impact or heavy financial burden against other nation-states, at a very low relative cost. As Dr. Gregory Falco notes, an attack against a satellite is possible for as little as $1000-$2000[64]. When further combined with the difficulties of international law, space based systems are prime targets for nation-states.

Overview of international law

Sources of law

Generally

To grasp the difficulties of some facets of international cyber law as a whole, a general understanding of international law can be seen as useful, given its much more complex nature compared to national law. In general it can be said that "The Charter of the United Nations (UN Charter) is the foundational document for the international legal system"[65], and while this may be true there is an inherent issue to understand regarding this.

[64] Falco, "Job One for Space Force: Space Asset Cybersecurity"
[65] Georgetown Law, "Guide to the Basics of International Law."

International law as a whole is undoubtedly quite difficult for a number of reasons; sovereignty of nations, consensus, lack of enforcement mechanisms, non-state actors just to name a few, but one of the biggest problems is the 'codification' of international law, or lack of it.

International law is primarily derived from a very finite amount of sources. These sources can be found in Article 38(1)[66] of the Statute of the International Court of Justice (ICJ).

- International Conventions
- International customs
- General principles of law
- Judicial Decisions & scholarly writings

The inherent problem with international law that is confusing to those generally familiar with domestic law is that "there is no single international government that creates and enforces international law"[67], thus it is decentralized in nature. Not only is there no clear law making or enforcing body, there is also no structured hierarchy that many are used to in domestic law.

International conventions

International conventions are the clearest of the three primary sources of international law and are formal agreements between states that are binding, which set out specific legal obligations for example, treaties. Even so there are very few binding conventions, the Budapest Convention on Cybercrime realistically being the only one as of December, 2023. There are other conventions that can and do apply to international cyber law, some of which will be talked about, but the Budapest convention is the only one that expressly details anything in the cyber sphere. All others are interpretations of existing law or simply non-binding. Further, there are no international conventions specifically for space cyber law.

[66] ICJ, "Statute of the International Court of Justice."
[67] Teach International Law. "How is International Law Created?"

International Customs

Unlike the previously mentioned international conventions, international customs are more prevalent in international cyber law, but less prevalent then the following general principles of law. International customs are still being developed for the cyber, and space-cyber sphere as customary law are the "international obligations arising from established international practices"[68](combined with Opinio Juris). As the internet itself is relatively new, so are the cyber attacks, weapons, and conflicts that come with it, thus customary laws are continually evolving. When this becomes intertwined with space based systems there is practically no Opinio Juris.

General Principles of law

General principles of law, while more present than their two aforementioned counterparts, are less codified and take more application to utilize. General principles of law are generally described as laws that "are commonly recognized as the norms existing in the municipal law of the majority of nations. When such a norm (i.e. the rule against judicial bias) has achieved the requisite degree of usage, it may thus be recognized as a subsidiary source of the substantive content of international law."[69] These principles are thought to be more of abstract concepts that provide a broad framework for legal interpretation. In terms of both cyber, and space-cyber law, ideas such as Sovereignty, Non-intervention, and Proportionality among many others are the basis used to determine where something sits. It is also important to international cyber law as it can be used as the basis for filling gaps where treaties or customs do not exist. This is important because of the novelness we not only see in cyber weapons, attacks, and conflicts, but the internet and cyberspace as a whole.

Judicial Decisions & scholarly writings

This source of law in itself is non-binding and not a primary source like the previous three. What it makes up for is the utility behind it. The previously referenced Tallinn Manual is a great (and

[68] Cornell Law School, "Customary International Law."
[69] "General Principles of Law"

one of the only few) sources to understand how existing international law can be applied to the cyber sphere in areas like conflict & warfare, as well as the MILAMOS is helpful for applying international law to space. The problem with this is it is not an official document but instead a (non-binding) academic study. While it is great for interpreting law and applying it to the cyber world, that is simply all it is relevant for. This is a common problem seen throughout the international legal system. It is very difficult to turn ideas into codified law, compared to the domestic level. While it is non binding, it addresses many of the later discussed topics (and seeks to interpret international cyber law just as we are), so it will be referenced quite extensively.

Space Cyber Law

International law itself is difficult, and international cyber law even more so, so when it comes to international space cyber law, it's apparent why there is little codified law to directly look to. Not only is it a facet of international law, but it is in both the cyber realm, which is inherently more uncertain and contains less contextual history to draw from than its counterparts, but then the layer of space is added, meaning even less context to draw from than the previous.

3.4 International Law, Cyber War, and Space

Clarification

Before diving in, just a quick clarification on words used. Some people argue that “Cyber-war is a highly problematic, even a dangerous, concept. An act of war must be instrumental, political and potentially lethal, whether in cyberspace or not. No stand-alone cyber-offence on record meets these criteria”[70] while others such as the International Committee of the Red Cross strictly use and define the term Cyber Warfare in a much broader context towards all cyber

[70] Valeriano, Maness, "Persistent Enemies and Cyberwar,"

conflicts, be it attacks or all out war. In terms of the following sections, cyber war and cyber conflict will be used relatively interchangeably.

Further Clarification

To also reiterate and expand on a previously mentioned point, according to Rule 112 in the MILAMOS, “Cyber activities that constitute space activities, including military space activities, are governed by international space law, as well as the applicable rules of general international law.”[71] To expand upon this reasoning, Article III in the Outer Space Treaty of 1967 identifies that international law applies to space activities and further in a 2012 Report by the UN Group of Governmental Experts it was found that international law applies in cyberspace. Through the transitive property, it can then be confirmed that international law applies to space cybersecurity. So for context in the following discussion, any basis in which cyber activities are being discussed, even if not outrightly said, the same can generally be said about space cyber activities.

Cyber vs traditional war (and beyond)

As we are comparing aspects of the cyber sphere with their counterparts in the real world it is only natural to look at traditional and cyber conflict as well.

As already seen thus far, cyber attacks have grown increasingly popular with nation-state actors as tools to push their agendas, without ‘muddying the water’ nearly as much as their traditional kinetic counterparts for a number of reasons. One of which is that they are not necessarily seen as committing an attack to the extent at which would be constituted as breaking international law. Or to better put it, “For state actors, the cyber domain is fast becoming the weapon of choice and is a “short of war” means to pressure other governments, manage conflict, impose costs on leaders and project national power.”[72]

---

[71] Jakhu and Freeland

[72] Foreign Policy Analytics, "The Rise of State-Sponsored Cyber Attacks and the Cost of Inaction,"

An ICBM launched at a target within the US would lead to a full scale conflict, but with malicious actors becoming more skilled at launching cyber attacks, the same effect could take place without the fear of escalation. The same can be said about space based attacks, such as an Anti-Satellite weapon (ASAT) launch. Launching an ASAT against a foreign nations satellite would very likely lead to an escalation of conflict and justification for the receiving country to retaliate. On the other hand, just like terrestrial based cyber attacks, cyber attacks launched against space assets generally would allow for plausible deniability by the launching country.

Defining cyber war

As previously discussed in the section *Defining Cyber Weapons*, some weapons are allowed in war and others are outright banned. The difficulty with this notion is oftentimes cyber weapons are not used nor cyber attacks carried out, in war. Just like how cyber weapons are difficult to define, so are cyber conflicts, wars, and attacks. Even though it might seem easier to define cyber warfare than cyber weapons, that does not mean it isn't a challenge as well. David Bloxberg writing for the A10 network says that "cyber warfare isn't as easy to define as conventional warfare. The reason? Cyber warfare is not about the acquisition of physical territory or the movement of troops and equipment, although it may support conventional warfare in achieving such objectives; it's about gathering intelligence, financial gain, damaging digital and physical infrastructure, hindering communications and the theft of intellectual property."[73] This leads us to trying to best define cyber war, but before that, let's briefly look back at space.

Cyberwar, in space?

For space cyber war, there has yet to be seen as a full scale conflict, but the previously mentioned ViaSat incident at the start of the Ukraine war can be seen, to some at least, as the first 'space-cyber war'. "The war in Ukraine saw, for the first time, the targeting of space assets

[73] A10 Networks, "Cyber Warfare: Nation State-Sponsored Cyber Attacks"

as part of a military campaign, not just using space to support other domains. It started with a Russian cyberattack on Viasat, a U.S. commercial space company, on the eve of its full-scale invasion of Ukraine, and continued with both parties launching cyberattacks on the space assets of their respective enemy. Indeed, the Ukraine war marks the arrival of warfare in space and, significantly, cyber warfare on space assets. If the Gulf War of 1991 was called the "first space war", the war in Ukraine has already been dubbed the first "space-cyber war""[74]

No definition?

Going back to definitions, in international law there is no standard, legally binding definition of war just as there is no standard definition of cyber, nor space-cyber war. The International Committee of the Red Cross (ICRC) defines Cyber warfare as "the means and methods of warfare that rely on information technology and are used in situations of armed conflict."[75], while this is beneficial, it is not a legally binding definition. This is the same for the Tallinn Manual as in Rule 103 - Definitions of means and methods of warfare, where cyber weapons and warfare are defined respectively as the "'means of cyber warfare' are cyber weapons and their associated cyber systems; and 'methods of cyber warfare' are the cyber tactics, techniques, and procedures by which hostilities are conducted."[76] While this is even more helpful for defining and understanding cyber warfare it still somewhat lacks clarity as to what extent legally constitutes cyber war.

In reality there isn't any concrete definition for cyber war, nor will there likely ever be.

In order to further formulate our understanding, what we can instead look to, just as the authors of the Tallinn Manual and generally those that practice international law might, is currently existing, codified, international conventions. Conventions such as the UN charter and the Geneva Convention. These detail the ideas of *jus ad bellum* and *jus in bello,* or the laws of

[74] Tepper et al.
[75] (Keep the second part of this definition in mind for the use of cyber weapons in peacetime.)
[76] Rule 103 Tallinn Manual

resorting to war and the laws in war itself[77], which can be used to create a more concrete understanding of how international law applies to cyber war.

We can begin to see how the previously mentioned 'sources of international law' begin to interact. The applicability of the charter and other binding sources of law are discussed in scholarly writings[78] such as the Tallinn Manual (seen above) and by the ICRC. When discussing and defining war, both in the real and cyber context, a key article that is often brought up is Article 2(4) of the UN charter, the guiding principle behind *jus ad bellum*. This article reads that "*All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.*"[79] This may sound quite ambiguous to be the most looked too stance/position/law dealing with international war ever created, but the reason behind this is that "Prior to the creation of the Charter, the use of force largely wasn't codified into law and the "resort to war was not initially prohibited" (1059), until the mid-20th century. From Schachter, International law in Theory and Practice (ch. 15 Sec 2, A. Basic Prohibition on the Use of Force) , we learn that the primary intention of the framers was to outlaw the classic definition of war (although the actual word war was never used) or as the Charter put it, "force", as this wording had a more encompassing scope of meaning."[80] and further "an important note is made at the bottom of page 1075 (Damrosch & Murphy) in that the words "war" and "aggression" were never used in the drafting like previous efforts, as the framers believed that these terms could be circumvented. Thus the word choice of "force." For instance, there could be some form of hostilities between nations that wouldn't amass to that of an all out war, the framer's intention was to halt this as well. In terms of hacking or a cyber-attack, it might not be an all out act of war executed by a nation, but it still could carry out a hostile act large enough

[77] Generally just described of as the 'laws of war' with the differentiation being made for clarity
[78] principle 4 of ICJ article 38(1)
[79] Article 2(4)
[80] Murphy, "Jus ad bellum and solar winds attack"

that it would constitute a use of force."[81] The challenge then is two fold, first what if a hostile act is not *per se* large enough to constitute an and how do we then regulate these varyingly scaled attacks.

3.5 Application & Its Challenges

It is already difficult to come to a consensus when it comes to simple definitions in the cyber sphere, as well as why applying international law is difficult, but this further becomes convoluted with more complex issues in the international cyber sphere. Below, a few common problems in relation to cyber weapons, attacks, and conflicts are detailed.

Threshold

While we begin to have a somewhat clear definition of war (although still quite indefinite), a question that many still have when it comes to cyber war is, what is the actual threshold for a cyber attack to be considered an act of war, as well as how do we deal with attacks that do not rise to this level. The notion of determining the use of weapons and its difficulty has been reiterated throughout this paper, and determining what degree actually constitutes their use is no different. This is discussed by the ICRC stating "The debates on whether a cyber-attack may amount to a "use of force" or even an "armed attack" under the UN Charter, which are ius ad bellum issues, are distinct, but parallel to the question of whether a cyber-attack alone can trigger the applicability of the IHL of international or of non-international armed conflicts. Determining the beginning of an armed conflict itself remains tricky in situations where cyber-attacks are employed alone, short of any kinetic use of force. It is argued that the respective traditional thresholds for international and non-international armed conflict should also be applied in such situations." And further posing the question, "Do cyber attacks amount to "attacks" in the sense of Article 49 of Protocol I? Is it necessary for them to result in physical

[81] Murphy, "Jus ad bellum and solar winds attack"

consequences such as destruction of objects or injury or death of persons?"[82] This is a serious problem that remains in cyber attacks. More often than not they do not cause serious injuries to people or things, yet are still very detrimental to society, so how do we regulate them? As of now this question remains unanswered.

Use in peacetime

Next when it comes to the overarching cyber war (or cyber use of force), legitimately viewed cyber conflicts (as in those that amount to a use of force or an act of war), in the eyes of the law, are much easier to interpret with international law than other areas of cyber war. Where international law really begins to break down is not during an evident cyber-conflict or as part of a "hybrid" war but instead in times of peace. Because cyber attacks often might not constitute a use of force and are just "short of war" the general rules around war do not apply which can be very difficult to regulate, especially when two nations are not at war with each other. Take for instance "in the past year alone, intelligence-gathering attacks to acquire vaccine-related IP have been linked to China, Russia and North Korea; Chinese state-sponsored surveillance operations and espionage efforts targeted pro-democracy organizations and individuals in Hong Kong; and unattributed ransomware attacks spread across more than 400 hospital and healthcare facilities in Puerto Rico, the United Kingdom, and the United States, causing an estimated $67 million in damages." None of these would constitute an attack great enough to be proportionally similar to a 'use of force' yet all of these are still very detrimental to a nation. As FP Analytics put it "Perhaps as worrisome as the attacks themselves is their frequent and increasing use during peacetime, when rules of engagement and international humanitarian law do not clearly apply"[83] As earlier discussed with the International Committee of the Red Cross' definition of Cyber warfare where it was stated that something is constituted as cyber warfare when "the means and methods of warfare that rely on information technology and are used in

[82] International Committee of the Red Cross. "Fundamentals of International Humanitarian Law (IHL)."
[83] Foreign Policy Analytics, "The Rise of State-Sponsored Cyber Attacks and the Cost of Inaction,"

situations of armed conflict." The second part of the definition "used in situations of armed conflict" is troublesome, as oftentimes situations do not amount to armed conflict but still are a serious burden. While this is problematic as state attacks can slip past the currently standing international laws, this is the inevitable current reality of the international landscape.

Who is responsible?

The question of where the responsibility falls internationally, for both the malicious acts that take place as well as who can reprimand the malicious actors is a question tirelessly brought up. For all intents and purposes let's say that laws specifically around cyber weapons, attacks, and conflict are actually codified into law, be it through treaties or even ramifications to the UN charter, there are still two inherent problems; attribution and enforcement.

Attribution

Technology itself makes determining who the malicious actors are very difficult. This is reiterated by the ICRC when discussing cyber war and holding attackers responsible, "Even then, in practice, the nature of information technology often makes it difficult to attribute an attack to a State or to an armed group (which is important to differentiate international from non-international armed conflicts) or to determine the existence of a sufficiently organized armed group (which is necessary to trigger IHL of non-international armed conflicts)."[84]

While the distinction as to what constitutes a cyber war or even a cyber attack remains a challenging question, due to the scarcity of comprehensive research as well as its recent emergence in the international community, the use of technology itself poses an even more inherent set of problems. This is "because cyber warfare is virtual and doesn't involve or require any kind of overt declaration of war, it's usually very difficult to prove that a particular state actor is responsible"[85]. As cyber war lacks physical boundaries as well as the traditional signs of an

[84] International Committee of the Red Cross, "Conduct of Hostilities."
[85] A10 Networks, "Cyber Warfare: Nation State-Sponsored Cyber Attacks"

attack, it is hard for a nation to even know they have been attacked, let alone who is attacking them. Imagine the following hypothetical: you're a soldier on a military base in your home country, when all of a sudden a missile appears out of thin air and blows up part of the base right in front of you. Initially all you might know is that an attack took place, later on once you've collected yourself and ensured there are no more missiles heading towards you, you can then start to discern who it was that launched this missile. Maybe look at the components that are remaining and try to match them with known missiles of your enemies, but what happens when even then, just as quickly as the missile appeared the majority of it also disappeared, only leaving you with mere scraps. They can be used to trace back the origins, but this is even more difficult. This very same scenario happens constantly in the cyber realm. Adding the step of space to it makes it even more complicated due to the very nature of space technology itself and how information is transmitted between the ground and space. Imagine the same scenario of the 'missile', but now when you go to look at the 'missile' it is traveling at 17,000 mph and 124 miles away from you.[86] While this may be a bit more dramatic than the reality, it's goal is to highlight the inherent difficulties of working with space based assets. Now going back to the hypothetical again, it becomes even convoluted when tracing the 'missile' back and it was launched not by a known enemy nation but by a non-state actor (or at least alleged).

Role of non-state actors

Non-state actors pose a very difficult problem when it comes to cyber warfare.

This can be seen as stated in Rule 33 of the Tallinn Manual as, "International law regulates cyber operations by non-State actors only in limited cases." and "Apart from specific areas of the law directed at the rights and obligations of individuals or other non-State actors (as in the case of human rights law, the law of armed conflict, and international criminal law), international law by and large does not regulate cyber operations conducted by non-State actors, such as

[86] Orbital Velocity of a LEO satellite, https://science.howstuffworks.com/satellite6.html

private individuals or companies."[87] This poses serious difficulties for reprimanding states as oftentimes what happens is 'non-state' actors can be used as proxies for state actors.

To highlight this problem take for instance the semi recent solar winds attack. In a paper on *Jus Ad Bellum and the Solar Winds Attacks* it is said that, "These attacks [solar winds] were perpetrated by the Russian SVR. The SVR is Russia's external intelligence agency, who were previously known as the KGB prior to the fall of the Soviet Union and subsequently have undertaken the role of the KGB. The SVR, which has been formally named as the instigators of the SolarWinds attack by the Biden administration, comprises three groups; APT 29, Cozy Bear and the Dukes. The issue in this lies in the fact that not only has Russia denied any and all claims, the SVR is also seen as a "civilian" intelligence agency. This is a common problem when it comes to cyber-warfare as oftentimes the origin of the attack is hard to trace."[88], while later in the paper this claim is refuted based on the fact that the international community had a high level of certainty it was Russia, this illustrates a very real problem within cyber warfare. With the use of VPNs, proxy servers, botnets, fast flux networks, SSH tunnels, P2P networks, and even dead drop resolvers, among many other means to spoof, hide, or make one's malicious virtual activity difficult to trace, in general it can be very hard to discern where an attack came from, let alone the question then if that entity is also affiliated with a state actor. This combined with the fact that state sponsored attacks are going to have a very sophisticated level of technology and vast amounts of resources available, it is near impossible to say beyond a reasonable doubt that the attack came from a specific country, especially compared to that of kinetic attacks.

Difficulty in enforcing

Going back to the SolarWinds attack, very little was actually done in response to Russia. First because of the severity of the attack. As cyber espionage is not regulated under international law and other aspects of the attack were not grand enough that a physical one of the same

[87] Rule 33 1 Tallinn Manual

[88] Murphy, "Jus ad bellum and solar winds attack"

proportionality would be considered a breach of international law. Secondly, and looking to the more overarching context of international law (instead of hyper-specific cyber law), international law is just generally hard to enforce.[89] Even so, as of 2023 there has never been a cyber attack that has resulted in physical death, and because of this many international laws have not gone into effect, as many experts agree for a cyber attack to be definitively seen as an act of war, it must have the same proportionality to one committed in the real world, such as people dying or buildings blowing up. But in the future say a cyber attack does result in physical damages to people or objects proportional to that of a traditional kinetic attack, the problem still remains that generally "international law cannot be enforced"[90] as "The absence of an international state means that international law relies principally on complex enforcement mechanisms, as opposed to a single powerful law enforcer. The focus is thus on the design and operation of enforcement mechanisms under conditions of decentralized power and authority."[91] There is no real means of enforcement at least to the extent that there should be, and this among many other problems in international cyber law, is not going away any time soon.

No UNified Council

The last challenge in the current context of international space cybersecurity law might be the most problematic, yet easily fixable. The UN currently addresses cyber security and space policy via two different channels. "Cyber: Groups of Governmental Experts (GGEs) on cybersecurity; Open-ended Working Group (OEWG) on cybersecurity

Space: GGE on Transparency and Confidence-Building Measures in Outer Space; agenda items of the prevention of an arms race in outer space (PAROS); OEWG on Reducing space

[89] It's important to note that cyber incidents like the SolarWinds attack often result in complex and multifaceted responses rather than direct or immediate punitive actions, especially when they involve major world powers. The responses tend to be more focused on improving defenses, diplomatic signaling, and establishing norms in cyberspace, rather than direct retaliation.

[90] Kirgis, "Enforcing International Law."

[91] Stephan, "Enforcement of International Law"

threats through norms, rules and principles of responsible behaviours."[92] The inherent problem with this is that it greatly restricts the sharing of information, and communication is a fundamental for creating adequate policy.

4. Suggestions

National Level

Compared to the international level, the steps that should be taken at the national level are relatively easier. While they might be seemingly easier, there are three crucial steps that should be taken to further our collective security.

1. Deem satellite systems their own piece of critical infrastructure, not just as part of it.
2. Enact binding laws of best practice that satellite operators and developers must follow. These binding laws should place safety, and thus cybersecurity more than anything at the forefront.
3. Create a shared lexicon of definitions pertaining to space cybersecurity

International Level

There are quite a number of routes that could be taken which could improve many of the aforementioned difficulties (but the question of whether they are feasible or not is another story). A unified council is the best overarching solution to many of the aforementioned issues, and this could be done in a number of ways.

New UN Council

The most powerful, but simultaneously difficult solution to this would be to add a seventh organ to the current six principal organs of the UN. This would be highly unlikely as the last of the six organs to be added was the ICJ in 1945 and it would require a restructuring of the charter, with approval from ⅔rds of the general assembly as well as all permanent members of the security

[92] Tepper, "Week 2"

council. While difficult and highly unlikely, because we are so heavily reliant on technology I believe this could be a very necessary step, especially in the future, as it would give the council a significant amount of authority and autonomy.

This new ‘organ’ would be called the United Nations Technology Council (UNTC) which could encompass everything tech related from practical implications to ethics, while also having a subcommittee for something along the lines of cybersecurity and cyber war.

Aside from this highly unlikely solution, there are three possible other options.

1. A specialized agency that works autonomously with the UN. This would by far be the easiest option, but these agencies are not governing bodies and would lack the authority to remedy many of the presented problems, only being able to coordinate with existing organs.
2. A Subsidiary Organ of either the General Assembly or Security Council, similar to that of the Human Rights Council. The UNTC would instead operate under one or both of the previously mentioned, already existing principal organs. Under the general assembly it could cover a broad scope of technology related issues, and under the security council it could focus more on the aspects and implications of technology on international peace and security.
3. A more collaborative Cross-Organ Structure, similar to the Peacebuilding Commission or the Counter-Terrorism Implementation Task Force, would be the best possible feasible approach. It would work as the following:

a. The core council of the UNTC would be composed of representatives from key UN principal organs (like the General Assembly, Security Council, and ECOSOC), specialized agencies (such as ITU, UNESCO, UNIDO), and relevant programs and funds (like UNDP, UNICEF). It could also include experts from non-UN entities such as international technology companies, academic institutions, NGOs, and civil society organizations focused on technology and digital rights.

b. Along with this it could have subcommittees on cyber warfare, digital development, and ethics/regulation. Specifically, the Cyber Warfare sub committee could deal with the strategic, legal, and security aspects of cyber warfare, coordinating closely with the Security Council and relevant agencies like UNODA (United Nations Office for Disarmament Affairs)

5. Conclusion

In concluding this paper, it's crucial to acknowledge that space cyber warfare introduces an additional layer of complexity and urgency to the already intricate domain of cyber conflict. The digital age has ushered in an era where cyberattacks transcend national borders and impact global infrastructure, and the inclusion of space assets only exacerbates these vulnerabilities. Satellites and other space-based systems are not only expensive and technically challenging to develop, but they also serve critical roles in communications, navigation, and defense. The very nature of space operations makes them attractive targets for state and non-state actors alike, as evidenced by incidents such as the ViaSat attack, which represents a new paradigm in space-cyber warfare.

Space cyber warfare necessitates rethinking the frameworks that guide international law and ethics. While traditional cyber weapons and attacks already pose challenges to international norms and regulations, the expansion into space creates a need for new standards that address the unique risks of this domain. Current laws governing cyber conflict, often grounded in principles of sovereignty and non-intervention, struggle to adapt to the multifaceted threats posed by space-based cyber weapons. The anonymity of cyber actors, the involvement of non-state entities, and the lack of a universally

accepted lexicon for these threats complicate attribution, responsibility, and enforcement.

The emergence of space cyber warfare calls for a reinvigorated approach to international cooperation and governance. A specialized body, possibly within the UN, should be established to address space-cyber issues directly, promoting the development of standards, norms, and practices that recognize the interconnectedness of space and cyber operations. National efforts must also prioritize the protection of space infrastructure by treating satellite systems as critical assets and implementing binding cybersecurity regulations.

Ultimately, the path forward in space cyber governance demands a blend of resilience, adaptability, and an unwavering commitment to international peace and security. We must embrace innovative, dynamic solutions that keep pace with evolving threats, foster transparency and collaboration, and uphold ethical standards. Only through comprehensive global governance and renewed international collaboration can we navigate the rapidly shifting terrain of space cyber warfare and ensure a secure and peaceful digital future.

Sources

1. NASA. "Sputnik and the Dawn of the Space Age." https://www.nasa.gov/history/sputnik/index.html.
2. Tepper, Eytan, Scott J. Shackelford, James B. Romano, and Sergei Dmitriachev. "The Sixth Warfighting Domain? Governing the Space-Cyber Nexus." System Standards: Space Data Link Security Protocol, https://public.ccsds.org/Pubs/355x0b2.pdf.
3. Henry, Caleb. "AST SpaceMobile Discloses Further Satellite Delays and Cost Increases." SpaceNews, https://spacenews.com/ast-spacemobile-discloses-further-satellite-delays-and-cost-increases/.
4. Erwin, Sandra. "Rocket Lab to Build Military Satellites for Space Development Agency." C4ISRNET, https://www.c4isrnet.com/battlefield-tech/space/2024/01/08/rocket-lab-to-build-military-satellites-for-space-development-agency/.
5. Encyclopædia Britannica. "Satellite Communication: How Satellites Work." https://www.britannica.com/technology/satellite-communication/How-satellites-work.
6. Fritz, Christian, Benjamin Maus, et al. "SatSec: Evaluating the Security of Satellite-based Internet Services." https://publications.cispa.saarland/3934/1/SatSec-Oakland22.pdf.
7. Modenini, A., and B. Ripani. "A Tutorial on the Tracking, Telemetry, and Command (TT&C) for Space Missions." IEEE Communications Surveys & Tutorials, vol. 25, no. 3, thirdquarter 2023, pp. 1510-1542, doi:10.1109/COMST.2023.3287431.
8. NASA. "State of the Art of Small Satellite Communication." NASA Small Satellite Institute, Date. https://www.nasa.gov/smallsat-institute/sst-soa/soa-communications/
9. CSIS. "Earth Orbit 101." CSIS Aerospace, Date. https://aerospace.csis.org/aerospace101/earth-orbit-101/
10. Computer History Museum. "Timeline of Computer History." Computer History Museum, Date. https://www.computerhistory.org/timeline/computers/
11. NASA. "Sputnik and The Dawn of the Space Age." NASA, Date. https://www.nasa.gov/history/sputnik/index.html
12. NASA. "Explorer 1 Overview." NASA, Date. https://www.nasa.gov/history/explorer-1-overview/
13. UNOOSA. "Introduction to Outer Space Treaty." UNOOSA, Date. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html
14. The Conversation. "How the Internet Was Born: From the ARPANET to the Internet." The Conversation, Date. https://theconversation.com/how-the-internet-was-born-from-the-arpanet-to-the-internet-68072
15. Gazette. "History of Space Command in Colorado Springs: Timeline." The Gazette, 10 Dec. 2020, https://gazette.com/military/history-of-space-command-in-colorado-springs-timeline/article_5bd0a13c-3b46-11eb-bd91-43521f574012.html.
16. See 2
17. Kumite. "609 IWS." Kumite.com, 24 Mar. 2003, https://web.archive.org/web/20110713173649/http://kumite.com/2003/03/24/609iws/.
18. ScienceDirect. "Moonlight Maze." ScienceDirect, https://www.sciencedirect.com/topics/computer-science/moonlight-maze.

19. Council of Europe. "The Budapest Convention." Council of Europe, https://www.coe.int/en/web/cybercrime/the-budapest-convention.
20. Council on Foreign Relations. "Estonian Denial of Service Incident." Council on Foreign Relations, https://www.cfr.org/cyber-operations/estonian-denial-service-incident.
21. Stanford Center for International Security and Cooperation. "Stuxnet." Stanford CISAC, https://cisac.fsi.stanford.edu/news/stuxnet.
22. U.S. Government. "Cybersecurity Policy Recommendations." GovInfo, 2020, https://www.govinfo.gov/content/pkg/CPRT-116HPRT38136/pdf/CPRT-116HPRT38136.pdf.
23. RAND Corporation. "RAND's Perspective on Space Security." RAND, 2021, https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE329/RAND_PE329.pdf.
24. U.S. Space Force. "History." Space Force, https://www.spaceforce.mil/About-Us/About-Space-Force/History/.
25. Federal Register. "The National Space Policy." Federal Register, 16 Dec. 2020, https://www.federalregister.gov/documents/2020/12/16/2020-27892/the-national-space-policy.
26. Trump White House Archives. "Space Policy Directive-5: Cybersecurity Principles for Space Systems." The White House, 4 Sept. 2020, https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/.
27. Neff, Stephen C. Justice Among Nations: A History of International Law. Harvard University Press, 2014, p. 17
28. Oxford Public International Law. "Weapons, Prohibited." The Oxford Public International Law. Oxford University Press, 2021. https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e447
29. (adapted from Cyber-Weapons, McBurney, Rid)
30. Schmitt, Michael N., editor. "Rule 92." Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, Part V.17 Section 2
31. (footnote)
32. Jakhu, Ram S., and Steven Freeland, eds. McGill Manual on International Law Applicable to Military Uses of Outer Space: Volume I - Rules. Centre for Research in Air and Space Law, 2022.
33. (footnote)
34. (footnote)
35. Valeriano, Brandon, and Ryan C. Maness. "Persistent Enemies and Cyberwar: The Dichotomy Between the Cyber and Physical Domains." The RUSI Journal, vol. 157, no. 5, 2012, pp. 98–105. Taylor & Francis Online, https://doi.org/10.1080/03071847.2012.664354.
36. O'Gorman, Gavin, and Symantec Security Response. “Stuxnet Explained: The First Known Cyberweapon.” CSO Online, IDG Communications, Inc., 26 Mar. 2021, www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html.

37. Kushner, David. “THE REAL STORY OF STUXNET”, The Real Story of Stuxnet, IEEE Spectrum, 2013, https://spectrum.ieee.org/the-real-story-of-stuxnet
38. See 35
39. K. Atrey. “Managing trust in cyberspace” Google Books, Google, 2018, p. 403
40. "Duqu 2.0: Frequently Asked Questions." Kaspersky, Kaspersky Lab, https://media.kaspersky.com/en/Duqu-2-0-Frequently-Asked-Questions.pdf.
41. Schmitt, Michael N., editor. "Rule 32." Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, Part I.5.
42. ResearchGate. "Space Cybersecurity: Lessons Learned from The ViaSat Cyberattack." https://www.researchgate.net/publication/363558808_Space_Cybersecurity_Lessons_Learned_from_The_ViaSat_Cyberattack.
43. ViaSat Blog. "KA-SAT Network Cyber Attack Overview." Accessed April 28, 2024. https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.
44. See 43
45. The Register. "ViaSat spills on Russian attack." March 30, 2022. https://www.theregister.com/2022/03/30/viasat_spills_on_russian_attack/.
46. See 43
47. Murphy, Jackson. “Space-cyber post mortem”
48. See 43
49. TechCrunch. "ViaSat confirms Russian wiper malware used in cyberattack." March 31, 2022. https://techcrunch.com/2022/03/31/viasat-cyberattack-russian-wiper/?guccounter=1.
50. BleepingComputer. "ViaSat confirms satellite modems were wiped with AcidRain malware." Accessed April 28, 2024. https://www.bleepingcomputer.com/news/security/viasat-confirms-satellite-modems-were-wiped-with-acidrain-malware/.
51. MIT Technology Review. "Russia's hack of ViaSat satellite shook Ukraine." May 10, 2022. https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/.
52. See 47
53. (footnote)
54. SentinelOne. "AcidRain: A Modem Wiper Rains Down on Europe." SentinelOne Labs, 15 Mar. 2022, https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/.
55. PCMag. "Report: US Concludes Russia’s Military Was Allegedly Behind Viasat Hack." PCMag, 10 May 2022, https://www.pcmag.com/news/report-us-concludes-russias-military-was-allegedly-behind-viasat-hack.
56. United States, Congress. Communications Satellite Act of 1962. Public Law 87-624. 76 Stat. 419, 1962. https://www.govinfo.gov/content/pkg/STATUTE-76/pdf/STATUTE-76-Pg419.pdf.
57. United States, Congress, Senate. Satellite Cybersecurity Act. 117th Congress, 2nd Session, S.3511, 2022. https://www.congress.gov/117/bills/s3511/BILLS-117s3511is.pdf.

58. United States, Congress, House. Satellite Cybersecurity Improvement Act of 2023. 118th Congress, H.R.5017, 2023. https://www.congress.gov/bill/118th-congress/house-bill/5017/all-info.
59. The White House, Office of the Press Secretary. "Memorandum on Space Policy Directive-5: Cybersecurity Principles for Space Systems." The White House Archives, 4 Sept. 2020, https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/.
60. Plotnek, J., and J. Slay. "Space Systems Security: A Definition and Knowledge Domain for the Contemporary Context." University of South Australia, Adelaide, Australia.
61. Foreign Policy Analytics. "The Rise of State-Sponsored Cyber Attacks and the Cost of Inaction." Foreign Policy, 17 Aug. 2021, fpanalytics.foreignpolicy.com/2021/08/17/the-rise-of-state-sponsored-cyber-attacks-and-the-cost-of-inaction/.
62. See 61
63. Reuter, “Cyber Attacks on US Banks” https://www.reuters.com/article/us-cyber-banks-iduskcn1r32nj
64. Falco, Gregory. "Job One for Space Force: Space Asset Cybersecurity." Cyber Security Project, Belfer Center for Science and International Affairs, Harvard Kennedy School, July 2018, www.belfercenter.org/Cyber.
65. "Guide to the Basics of International Law." Georgetown Law, Georgetown University, 2019, www.law.georgetown.edu/wp-content/uploads/2019/08/A-Guide-to-the-Basics-of-Intl-Law.pdf.
66. Statute of the International Court of Justice." International Court of Justice, United Nations. https://www.icj-cij.org/statute.
67. Teach International Law. 'How is International Law Created?' Teach International Law, https://teachinternationallaw.ca/guide/what-is-il/how-is-il-created.
68. Cornell Law School, Legal Information Institute. 'Customary International Law.' Cornell Law School, Legal Information Institute, www.law.cornell.edu/wex/customary_international_law.
69. See 28, “General Principles of Law”
70. See 35
71. See 32
72. See 61
73. A10 Networks. “Cyber Warfare: Nation State-Sponsored Cyber Attacks - A10 Networks”, A10 Networks, www.a10networks.com/blog/cyber-warfare-nation-state-sponsored-cyber-attacks/.
74. See 2
75. (footnote)
76. Schmitt, Michael N., editor. "Rule 103." Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013
77. (footnote)
78. International Court of Justice. "Statute of the International Court of Justice, Article 38(1), Principle 4." United Nations, 1945. United Nations Treaty Series, vol. 33, no. 993, 1945. United Nations, treaties.un.org.

79. United Nations. "Charter of the United Nations, Article 2(4)." United Nations, 24 Oct. 1945, www.un.org/en/charter-united-nations/.
80. Murphy, Jackson. Jus Ad Bellum and the Solar Winds Attacks
81. See 80
82. International Committee of the Red Cross. "Fundamentals of International Humanitarian Law (IHL)." How Does Law Protect in War? - Online Casebook, ICRC, https://casebook.icrc.org/law/fundamentals-ihl#b_iii_1.
83. See 61
84. "Conduct of Hostilities." How Does Law Protect in War? - Online Casebook, International Committee of the Red Cross, https://casebook.icrc.org/law/conduct-hostilities#footnote91_pabssir.
85. See 73
86. (Footnote)
87. Schmitt, Michael N., editor. "Rule 31" Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013. 1
88. See 80
89. (Footnote)
90. Kirgis, Frederic L., Jr. "Enforcing International Law." ASIL Insights, vol. 1, no. 1, 22 Jan. 1996, www.asil.org/insights/volume/1/issue/1/enforcing-international-law.
91. Stephan, Paul B., 'Enforcement of International Law', in Francesco Parisi (ed.), The Oxford Handbook of Law and Economics: Volume 3: Public Law and Legal Institutions (2017; online edn, Oxford Academic, 10 May 2017), https://doi.org/10.1093/oxfordhb/9780199684250.013.034, accessed 8 Dec. 2023.
92. Tepper, Eytan. “Week 2”, Slides. Space Cybersecurity Digital Badge