Malicious Non-state Actors and Contested Space Operations

Report to the Office of University Programs, Science and Technology Directorate, U.S. Department of Homeland Security and the Strategic Multilayer Assessment Branch, Joint Staff/J-39 Directorate for Special Activities and Operations, U.S. Department of Defense

February 2018

National Consortium for the Study of Terrorism and Responses to Terrorism
A Department of Homeland Security Science and Technology Center of Excellence
Led by the University of Maryland

8400 Baltimore Ave., Suite 250 •College Park,MD 20742 • 301.405.6600
www.start.umd.edu

About This Report

The authors of this report are Rachel A. Gabriel, Researcher, and Barnett S. Koven, Senior Researcher, at the National Consortium for the Study of Terrorism and Responses to Terrorism (START). Questions about this report should be directed to Barnett S. Koven at bkoven@start.umd.edu.

This report is part of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) project, "Violent Non-state Actors and Contested Space Operations," led by Amy Pate and Barnett S. Koven.

This research was supported by the U.S. Department of Homeland Security Science and Technology Directorate's Office of University Programs, with funding provided by the Strategic Multilayer Assessment (SMA) Branch, Joint Staff/J-39 Directorate for Special Activities and Operations, U.S. Department of Defense, through grant award number 2012ST061CS0001-05 made to START. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the U.S. Department of Defense or START.

About START

START is supported in part by the Science and Technology Directorate of the U.S. Department of Homeland Security through a Center of Excellence program led by the University of Maryland. START uses state-of-the-art theories, methods and data from the social and behavioral sciences to improve understanding of the origins, dynamics and social and psychological impacts of terrorism. For more information, contact START at infostart@start.umd.edu or visit www.start.umd.edu.

Citations

Gabriel, Rachel A. and Barnett S. Koven. "Malicious Non-state Actors and Contested Space Operations," Report to DHS S&T Office of University Programs and DoD Strategic Multilayer Assessment Branch. College Park, MD: START, 2018.

Contents

Executive Summary

This report provides an analysis of potential threats to space-based systems posed by non-state actors. It places particular emphasis on the need to consider the space domain as part of a multi-domain threat environment where domains are interconnected and interdependent. This research devotes significant attention to examining the nexus between space and cybersecurity, and to the strategic vulnerabilities posed by the increasing integration of cyber and space technologies in critical infrastructure.

It proceeds by examining the nature of cross-domain threats, and the space-cyber nexus. It then provides an overview of potential space-based threats and risks. Subsequently, the report develops a typology of malicious actors based on their motives and capabilities. Importantly, this report evaluates the risks that each type of actor might pose individually or in concert with other types of actors. While some non-state actors with malicious intent possess the requisite capabilities to directly threaten space-based systems, many groups possess only malicious intent or the requisite capabilities – not both. Consequently considering non-state actor collaboration is especially necessary. This report also highlights how space-based capabilities, such as open-source satellite imagery, can be (and indeed, has been) exploited by non-state actors to further their terrestrial objectives. Finally, it concludes with some recommendations to increase resiliency.

In disaggregating threatening groups by motivation and capabilities, this report finds that of all the types of actors, cyber warriors backed by nation states have the greatest potential and interest to interfere in space. In contrast, more traditional violent non-state actors (VNSAs) have the most limited capability, and probably the smallest interest, in interfering in space. Despite this, it is clear that VNSAs do have much to gain by exploiting space-based technologies (e.g., for intelligence collection, propaganda) in support of their terrestrial activities.

While many of the scenarios contained in this report are largely hypothetical, they are possible. Specifically, at least some non-state groups already possess many of the requisite capabilities and malicious intent. Moreover, there are numerous known security deficiencies in commercial space technologies. As commercialization of the space domain and the number of new commercial entrants increase, existing vulnerabilities will become more pronounced, and additional vulnerabilities will be created. In short, the expansion of multinational commercial space operations is outpacing the ability of governments to anticipate or regulate activities in this domain. Moreover, as space-based capabilities become ever more important to economic activity and terrestrial infrastructure, they also become more attractive targets.

Introduction

The National Consortium for the Study of Terrorism (START) has been tasked with providing support to the Headquarters Air Force (HAF/A3), U.S. Strategic Command (USSTRATCOM) and Air Force Space Command (AFSPC) Contested Space Operations Effort undertaken as a Strategic Multi-layer Assessment initiative. This report addresses threats posed to U.S. space-based assets by non-state actors.

Space-based infrastructure is of critical importance to both the U.S. military and civilian sectors. Both are extremely reliant on space-based architecture for navigation, communication, etc. Consequently, cross-domain threats are especially likely. These can include kinetic or cyber-attacks on ground-based infrastructure (e.g., satellite ground control stations) for the purposes of damaging, destroying or denying access to military and/or civilian space-based capabilities. Inversely, they could involve attacks on space-based equipment (e.g., GPS navigation satellites, communications satellites) in order to hinder the movement of U.S. military forces or to disrupt civilian communications and associated economic activity. Therefore, this report examines both attacks perpetrated in non-space domains (land, sea, air and information) that intend to effect space-based capabilities, as well as attacks on space-based infrastructure for the purposes of affecting other domains. In addition, this report briefly examines the use of low-cost, commercially available space-based technology (e.g., high-resolution satellite imagery) used by terrorist and insurgent groups in perpetrating attacks.

Importantly, this research also explores how capabilities and intentions vary across different types of non-state actors. For example, sophisticated hacker groups are more likely to employ cyber-attacks (information) in targeting space-based infrastructure than insurgent and terrorist organizations, which tend to lack highly sophisticated cyber capabilities. Beyond capabilities, varying motives between different types of groups also affect their choice of targets. In addition, and where relevant, this report examines evidence of collaboration between various disparate group types (e.g. al-Qa'ida's collaboration with Russian cyber criminals). Threat resiliency is also discussed.

This report proceeds in five sections. The first overviews the importance of cross-domain security threats involving non-state actors. The subsequent section describes the more likely potential threats and vulnerabilities posed by these groups. The third section examines the capabilities and motivations of various non-state actor group types. The penultimate section explores resiliency to potential threats posed by these groups. The final section concludes.

The Nature of Cross-domain Security Threats Involving Non-state Actors

Recent literature evaluating the global security environment has emphasized the need to consider all security domains – including air, sea, land, space and cyber – in concert as interconnected and interdependent. This is the case given the increasing interdependence of all domains, especially with regard to technology and cyber capability. This is particularly true of space and the strategic vulnerabilities that are created by the interdependence of space and other domains. Both civilian and defense sectors are vulnerable to significant disruptions caused by threats to space-based systems. This section emphasizes the importance of considering multiple domains together and how inter-domain relationships between space, cyber and other domains have created strategic vulnerabilities to U.S. interests that might be exploited by potential adversaries, including malicious non-state actors (MNSAs).[1]

[1] We choose to coin the term malicious non-state actors, to underscore that violent non-state actors (VNSAs) are not the only type of non-state groups capable of exploiting U.S. vulnerabilities in space. For example, sophisticated hacker groups, cybercriminals and transnational criminal organizations that do not necessarily employ violence to achieve their objectives harbor malicious intent and the necessary capabilities to threaten U.S. security in space.

It includes a recent literature review on the new security environment. This covers discussion of space and cybersecurity threats to military and commercial interests and an analysis of their associated risks.[2] However, it also covers cross-domain relationships that exist between space and cyber, as well as other domains, and notes the strategic vulnerabilities to U.S. space-based infrastructure resulting from these multi-domain relationships.

Cross-domain operations are those that attack one (or more) domain(s) with the intention of causing an effect in an additional domain(s).[3] One example of this would be an adversary attacking U.S. GPS guidance satellites in order to impede navigation by U.S. naval vessels.[4] Alternatively, a cyber-attack on the power infrastructure[5] servicing satellite ground control stations could be employed to deny the U.S. commercial banking sector access to their satellite networks, potentially wreaking economic havoc.[6] In the former scenario space-based capabilities are attacked with the intent of degrading naval systems. In the latter scenario, ground-based power infrastructure is attacked in order to deny access to satellites. As such, it is necessary to examine both how space-based infrastructure creates vulnerabilities in other domains, as well as how vulnerabilities in other domains may adversely affect U.S. space control. Moreover, it is important to realize that in the former example, the adversary's desired end was to degrade U.S. military capabilities. In the latter case, the end was to damage the U.S. civilian economy. Both types of attacks can be hugely consequential.

Not only do cross-domain attacks have the potential to inflict serious damage, they can be perpetrated by MNSA's (or states) that lack the capability to directly cause comparable harm to a given domain. For example, U.S. precision strike capabilities have proven to be a critical tool for prosecuting the conflict against violent extremism.[7] While MNSA's lack integrated air defenses and naval surface-to-surface missiles, and are thus unlikely to be able to shoot down fixed-wing combat aircraft or sink cruise missile carrying naval vessels, a successful attack on guidance satellites would deny the U.S. military the ability to deploy these precision strike capabilities without having to destroy precision strike weapons or their delivery vehicles.[8] In the non-military realm, the idea that MNSA forces would conduct synchronized kinetic attacks against hundreds of banks simultaneously is outlandish. However, targeting satellite communications networks used by the commercial banking sector could still produce the same desired effects.[9]

Moreover, space will become an even more attractive target for MNSAs over time. This is the case for two reasons. First, U.S. forces already possesses a massive advantage – in terms of the technical capabilities, martial capacities, training, equipment, etc. – over MNSA adversaries. Successful MNSA forces recognize

[2] This report will use the term threat to refer to the combination of capability and intent required for an event to occur, and will use the term risk to refer to the probability that such an event might occur and the associated harm that would come from such an occurrence.
[3] Vincent Manzo, "Deterrence and Escalation in Cross-domain Operations," *JFQ: Joint Force Quarterly* 66 (2012): 8-14.
[4] Christopher Woody, "The Navy's 4th accident this year is stirring concerns about hackers targeting US warships," *Business Insider,* August 24, 2017, http://www.businessinsider.com/hacking-and-gps-spoofing-involved-in-navy-accidents-2017-8.
[5] Insofar as most ground control stations are air-gapped, direct cyber-attacks against these facilities are only possible if the attackers are able to gain physical access to the control station. However, power infrastructure servicing these stations, including network controlled backup generators, are vulnerable to remote cyber-attack.
[6] Dr. Dawie de Wet, "Satellite networks could prove key to the financial services industry," *Memeburn,* September 1, 2015, https://memeburn.com/2015/09/satellite-networks-could-prove-key-to-the-financial-services-industry/.
[7] David Livingstone and Patricia Lewis, "Space, the Final Frontier for Cybersecurity?," *Chatham House, International Security Department*, September 2016; Micah Zenko, "Dangerous Space Incidents," Contingency Planning Memorandum (Council on Foreign Relations: New York) 2014, 3).
[8] Zenko,"Dangerous Space Incidents," 5.
[9] de Wet, "Satellite networks."

that they cannot hope to compete conventionally with the U.S. armed forces; as such, they employ unconventional approaches such as insurgency or terrorism, which denies the United States the ability to bring the full weight of its military power to bear. They also repurpose low-cost technology that is difficult or expensive to defend against. (For example, the Islamic State has used hastily armored vehicles as VBIEDs. These have proven to be easy to build and exceedingly difficult to stop. In a sense, when combined with a suicidal driver, these vehicles are a low-tech, low-cost precision guided munition;[10] The Islamic State has also become proficient at adapting commercial, of-the-shelf drones to deliver ordinance).[11] As the capacities gap continues to widen, innovative MNSAs are likely to increasingly view space as an attractive new frontier.

Second, the consequences of a successful attack on space-based systems will only become more severe over time, as the pace of innovation in space technology and unregulated commercial demands for space offerings results in space becoming an inextricable part of daily life. If it is not already the case, soon the space domain and its ground elements will become permanently embedded in global infrastructure, which accounts for trillions of data transactions per day involving communications, navigation and timing, earth observation and other such necessities.[12] Furthermore, whereas space used to be the exclusive domain of highly sensitive and well protected military and intelligence satellites (as well as research satellites launched and controlled by governments), the profusion of low-cost, commercial satellites, as well as satellites designed, built and operated by students,[13] has introduced new, exploitable vulnerabilities.[14]

Potential Space Vulnerabilities and Threats

While cross-domain operations involving space, and targeting U.S. military or civilian capabilities are certainly appealing to state actors that are unable to compete with the United States in more conventional domains, the focus of this report is on threats posed by MNSAs. Therefore, only vulnerabilities that MNSAs are likely to exploit will be discussed. Whereas no MNSAs (and only four[15] states have viable kinetic anti-satellite weapons (ASATs)), numerous MNSAs already possess sophisticated and proven cyber capabilities. Consequently, the primary focus will be on the link between cybersecurity and space security, as well as other attack modalities that at least some MNSAs are capable of executing. In addition, this section will examine the use of space-based technology by MNSAs in the planning and execution of their own kinetic attacks. For example, various insurgent and terrorist

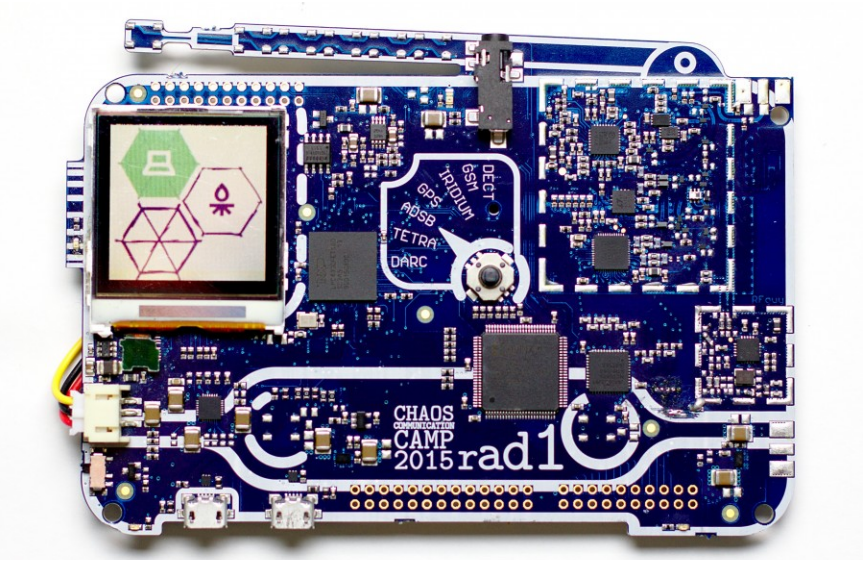
[10] Hugo Kaaman, "The History and Adaptability of the Islamic State Car Bomb," Blog Post, February 14, 207, https://zaytunarjuwani.wordpress.com/2017/02/14/the-history-and-adaptability-of-the-islamic-state-car-bomb/islamic.
[11] Nick Waters, "Types of Islamic State Drone Bombs and Where to Find Them," *Belingcat,* May 24,2017, https://www.bellingcat.com/news/mena/2017/05/24/types-islamic-state-drone-bombs-find/.
[12] Livingstone and Lewis, "Space, the Final Frontier for Cybersecurity."; UK HM Government (2014), "National Space Security Policy," UKSA/13/1292, p. 2, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307346/National_Space_Security_Policy.pdf.
[13] CubeSat's were envisioned as a way for graduate students to be able to design, launch and operate satellites for educational purposes. As of January 1, 2018, 811 have been launched (http://www.nanosats.eu/). In 2016, the St. Thomas More (STM) Sat-1 became the first satellite built by elementary school students to be deployed to space (https://www.nasa.gov/feature/first-cubesat-built-by-an-elementary-school-deployed-into-space).
[14] Hoshua Hampson, "The Future of Space Commercialization," Research Paper (Niskanen Center, 2017), https://science.house.gov/sites/republicans.science.house.gov/files/documents/TheFutureofSpaceCommercializationFinal.pdf.
[15] The United States, China and Russia have all successfully tested ASATs. In addition, Israel has completed an ASAT developed in partnership with the United States. India claims to be developing an ASAT capability, but most experts believe that India does not yet have a serious capability in these area (https://thediplomat.com/2016/06/indias-anti-satellite-weapons/).

organizations have taken advantage of low-cost, commercially available high-resolution satellite imagery in order to plan their attacks.

The Space-Cyber Nexus

As indicated, many of the most threatening cross-domain vulnerabilities exist in the nexus between cybersecurity and space-based systems. Satellites and other space assets, like other types of digitized critical infrastructure, are vulnerable to cyber-attack. Importantly, many space-based systems were designed before cyber-attack was a significant concern. These components are therefore especially vulnerable to new, sophisticated methods of cyber-attack. Commercial space-based capabilities are particularly vulnerable due to lower levels of encryption and security.[16] Moreover, the fact that the current pace of space technology innovation and production is outpacing regulation increases the likelihood of major security gaps.[17] As security expert David Ignatius notes, "as on Earth, the hidden danger is hacking….Orbits can be changed; sensors can be blinded; data can be corrupted. Facts could become as fragile in space as on Earth, if systems aren't protected."[18]

Let's consider a concrete example. The Iridium satellite network is a constellation of 66 low earth orbit communications satellites. Iridium's largest user is the U.S. Department of Defense. However, it is also used by journalists, extractive industries (e.g., oil, gas, mining), and by commercial airlines to track their planes. The network was designed in the 1980s and was obsolete from a cyber-security standpoint even before it began operating in 1998. Most communications traffic on the network is sent in the clear. Despite this, Iridium claimed "the complexity of the Iridium air interface makes the challenge of developing an Iridium L-Band monitoring device very difficult and probably beyond the reach of all but the most determined adversaries."[19] Nevertheless, two hackers at the annual Chaos Communications Camp meeting in 2015 demonstrated the ease of doing so. The full, 46-minute video of their demonstration is available on the conference website, all of their computer code can be downloaded from GitHub, and the only hardware



Source: "Rad1o to hardware overview," https://rad1o.badge.events.ccc.de/hardware:overview

[16] Matt Burgess, "Hackers targeting satellites could cause 'catastrophic; damage," *Wired,* September 22, 2016, http://www.wired.co.uk/article/satellites-vulnerable-hacking-chatham-house.
[17] Tarek Saadawi and John Colwell, Jr. *Cyber infrastructure Protection Volume III* (Carlisle:Army War College-Strategic Studies Institute Carlisle United States, 2017), 15.
[18] David Ignatius, "War in Space is Becoming a Real Threat," *The Washington Post,* March 16, 2017 https://www.washingtonpost.com/opinions/war-in-space-is-becoming-a-real-threat/2017/03/16/af3c35ac-0a8f-11e7-a15f-a58d4a988474_story.html?utm_term=.c43d4ab32f5c
[19] J.M. Porup, "It's surprisingly simple to hack a satellite," *Motherboard,* April 21, 2014, https://motherboard.vice.com/en_us/article/bmjq5a/its-surprisingly-simple-to-hack-a-satellite; Iridium Hacking, Please don't sue us," https://media.ccc.de/v/camp2015-6883-iridium_hacking#t=1427; "Rad1o to hardware overview," https://rad1o.badge.events.ccc.de/hardware:overview

they used (in addition to a basic laptop PC) was a software-defined radio (pictured above), worth about US$50 (and given out for free in the conference grab bags to all 4,500 attendees).[20]

While the two presenters were simply interested in exposing a glaring vulnerability, it is not hard to see how this capability could be leveraged by MNSAs. Indeed numerous hacker groups have focused extensively on hijacking commercial satellites to syphon off sensitive data. A particularly infamous group, Turla APT (Advanced Persistent Threat) has used similar techniques to syphon off sensitive U.S. and Chinese military and diplomatic data. They have also targeted industry. For example, they have stolen proprietary data from pharmaceutical companies.[21]

Beyond eavesdropping on satellite feeds, MNSA's are also capable of denying their opponents access to their own signals or altering the nature of those signals. One way in which this is accomplished is by jamming satellite signals. Jamming is defined as an "attempt to degrade and disrupt connectivity by interfering with the signals that are meant for communication."[22] Recent advances in the affordability and commercial availability of jamming technology has produced jammers that are relatively inexpensive (some GNSS jammers can be purchased online for less than US$50), easy to use, and continue to become smaller and easier to hide (many pocket-sized options are currently available). Types of jamming attacks include terrestrial jamming, such as Distributed Denial of Service (DDoS) attacks, that affect the operating ability of a receivers in a specific geographic region, and orbital jamming that interferes with the signal transmitted by a ground station. Terrestrial jamming has long been used by authoritarian regimes seeking to block specific radio or television broadcasts. More recently, terrestrial jamming has been employed to block cellular signals and internet access (called a wireless denial of service (DoS) attack). Indeed even disgruntled moviegoers, café owners and public transit commuters have used cheaply available terrestrial jammers to block cellphone service.[23]

Both types of jamming work by generating a signal that is at least slightly more powerful than the signal being broadcast by the satellite or ground control station.[24] Terrestrial jamming is relatively easy, since the objective is to use a ground-based signal generator to block receipt of a satellite signal by a ground-based receiver. While even relatively weak signals like GNSS used for GPS guidance are powerful close to the satellite from which the signal originates, by the time the signal reaches earth, it is weak. As such, terrestrial jammers, which benefit from proximity to the receivers, do not need to emit a strong signal to block communications.[25] That said, the range of a jammer is conditional on factors such as its power, atmospheric conditions, topography and the quality of the receiver.[26] As such, MNSAs wishing to jam communications over extended distances will need to invest in more sophisticated, larger and more expensive jammers.

---

[20] Porup, "It's surprisingly simple to hack a satellite."; Iridium Hacking, Please don't sue us," https://media.ccc.de/v/camp2015-6883-iridium_hacking#t=1427.
[21] Swati Khandelwal, "Russian Hackers Hijack Satellite to Steal Data From Thousands of Hacked Computers," *The Hacker News,* September 10, 2015, https://thehackernews.com/2015/09/hacking-satellite.html.
[22] Livingstone and Lewis, "Space, the Final Frontier for Cybersecurity?"
[23] Matt Richtel, "Devices Enforce Silence of Cellphones, Illegally," *The New York Times,* November 4, 2007, http://www.nytimes.com/2007/11/04/technology/04jammer.html; Kashmir Hill, "Jamming GPS Signals is Illegal, Dangerous Cheap and Easy," *Gizmodo,* July 24, 2017, https://gizmodo.com/jamming-gps-signals-is-illegal-dangerous-cheap-and-e-1796778955.
[24] Riyad Mitieb Mahmood, "The Mechanism of Deliberate Jammin on the Broadcast Satellite Service." *Journal of University of Anbar for Pure Science:* 6:2, 2012, 3, https://www.iasj.net/iasj?func=fulltext&aId=63233.
[25] Hill, "Jamming GPS Signals."
[26] Livingstone and Lewis, "Space, the Final Frontier for Cybersecurity?"

Unlike with terrestrial jammers where their efficacy is a function of power and distance from the receiver (among other, aforementioned factors), orbital jamming does not need to be located near the ground-based equipment it is attempting to interfere with.[27] Orbital jamming seeks to overpower the signal being transmitted from ground-control stations to satellites. Consequently, orbital jammers can be located anywhere within the receiving beam of the satellite. The ability to disrupt ground-satellite communications from afar would certainly be appealing to MNSAs. However, this requires the ability to broadcast strong signals. Consequently, orbital jamming is primarily the domain of states for the moment. Nevertheless, the Senate Armed Services Committee's 2016 Worldwide Threat Assessment acknowledges the current global threat from electronic warfare systems that are capable of jamming satellite communications and global navigation space systems. The report assesses that "this technology will continue to proliferate to new actors and that our more advanced adversaries will continue to develop more sophisticated systems in the next few years."[28]

Spoofing, another method of cyber interference, manipulates the content of communications and reduces its integrity. Unlike jamming, it can be applied at both the receiving and transmitting ends of a signal.[29] Whereas jamming simply requires disrupting the signal, spoofing requires an attacker to be able to understand and manipulate a signal. As such, it is unlikely that an MNSA could directly interfere with the content of encrypted military signals. Nevertheless, MNSAs may be able to break the encryption on commercial signals or spoof the myriad signals sent in the clear. For example, a spoofing attack might directly target and damage a national power grid by introducing false timing signals or cause indirect economic damage by targeting high-frequency systems of the financial services sector (e.g., electronic securities trading).[30] The ability to disrupt communications signals was demonstrated in 2013, when Dr. Tom Humphreys and a team of scientists at the University of Texas used a lab-built device to fake GPS signals that were slightly stronger than the authentic ones. They were able to take control of and reset a luxury yacht's satellite navigations system to lock on to the counterfeit GPS signal in a way that was invisible to the captain, causing it to falsely report that the vessel was off course. Unaware that the GPS was incorrect, the captain then adjusted course. Subsequently, in June 2017, the GPS navigations systems of 20 ships in the eastern Black Sea were manipulated to deliver false signals while appearing to function normally. Attacks later that month on thousands of computer systems disrupted shipping worldwide.[31] In fact, cybersecurity experts have recently discovered how frighteningly easy it is to hack into certain types of ship navigation equipment. The discovery resulted from the creation of a ship-tracking map, powered by data from Shodan,[32] which uses data from vessels' VSAT antennas to pinpoint real-time locations of ships around the globe. At least some ships use VSATS with public IPv4 addresses without any type of firewall, allowing them to be easily located. Shockingly, many of these VSATS default log-in credentials remain unchanged and are easily found online, allowing anyone to gain administrator-level access, manually change its GPS coordinates and even upload their own firmware. With a simple google search, an attacker can determine a great detail about the vessel in question, for example if it contains a "secure, sealed, climate-controlled armory," the implications of which would be of obvious interest for an MNSA.[33] While the number of vessels that can be so easily hacked is obviously limited, the fact remains that

[27] Mahmood, "The Mechanism of Deliberate Jamming on the Broadcast Satellite Service."
[28] Director of National Intelligence James Clapper, "Worldwide Threat Assessment of the US Intelligence Community," Senate Armed Services Committee, (Washington, D.C., 2016.)
[29] Mahmood, "The Mechanism of Deliberate Jammin on the Broadcast Satellite Service."
[30] Livingstone and Lewis, "Space, the Final Frontier for Cybersecurity?"
[31] Woody, "The Navy's 4th accident this year."
[32] Shodan is a search engine that allows users to search for internet-connected devices. It is heavily used for information sharing by hackers.
[33] Jack Morse, "Remotely hacking ships shouldn't be this easy, and yet ...," *Mashable,* July 18, 2017, https://mashable.com/2017/07/18/hacking-boats-is-fun-and-easy/#KYk3Hm5Q_aqf.

MNSAs seeking to exploit GPS satellite technologies have numerous avenues to do so. The implications of this type of attack for a large, crude carrier operating in confined waters, or any other type vehicle reliant on GPS navigation could be devastating.[34]

The failure of modern commercial satellite companies to re-engineer archaic and insecure systems vulnerable to hacking, jamming and spoofing can have serious consequences that range from theft of valuable or dangerous cargo to loss of life. For example, in 2015 security researcher Colby Moore demonstrated that satellite tracking technology sold by GlobalStar, one of the world's largest providers of satellite voice and data communications, could be easily and cheaply hacked using a receiver made from similar off-the-shelf components to those in the aforementioned Iridium example. GlobalStar markets its asset-tracking systems to industries ranging from oil and gas, to aviation, and to the military, with over 150,000 units in use worldwide. In addition to cargo and asset-tracking, the company markets personal tracking devices, used in search-and-rescue missions, as well as trackers used in SCADA environments to monitor critical infrastructure projects, such as pipelines and oil rigs, where phone and internet signals are out of reach. All of these technologies rely on the same unencrypted data network, Simplex, to send data between transmitters, satellites and ground stations, allowing for interception, jamming or spoofing of communications. Problematically, authentication of communications is not required to ensure that only legitimate data is transmitted. Moore was able to easily re-engineer the protocol underlying Simplex to determine that all GlobalStar devices use the same code to transmit data, allowing him to create his own code. Anyone capable of using a similar receiver would be able to identify where the trackers are located, and could hijack or spoof the data so that it appears to be on course. For example, an MNSA hijacker could track highly valuable or dangerous cargo, such as electronics, gas, chemicals, military equipment or even nuclear materials, disable the location-tracking device, and then spoof the coordinates so that the hijacked cargo appears to be on course. MNSAs could similarly exploit security vulnerabilities to interfere with critical infrastructure systems or human-tracking efforts. Blue force tracking could also be accessed by adversaries in order to help them avoid or target U.S. forces.[35]

A less dramatic but still detrimental attack might target banks and stock exchanges. Criminal elements seeking financial gain might employ similar approaches to intercept and manipulate content for financial gain. For example, a sophisticated cybercriminal might spoof securities markets by targeting GNSS timing functions, which automatically insert time stamps on transactions.[36] In doing so s/he can backdate his/her own trades to commit wire fraud. A sophisticated MNSA could use a similar approach to fund itself, or on a wider scale to undermine confidence in a securities market. Indeed, risks to the financial sector have increased as financial service providers have increased reliance on satellite communications. Ironically, this move was motivated by increased cyber threats to terrestrial financial infrastructure (as well as declining costs and increasing reliability of space-based alternatives).[37]

An additional threat involves cyber, kinetic or integrated cyber-kinetic attacks on ground control infrastructure. For example, cyber and/or kinetic means could be used to attack grid and auxiliary power servicing a ground control station, thereby impeding the ability of the site to communicate properly with a satellite. For example, hackers have already demonstrated the versatility of DDoS attacks, which have

[34] Woody, "The Navy's 4th accident this year."
[35] Kim Zetter, "Hackers Could Heist Semis by Exploiting This Satellite Flaw," *Wired,* July 30, 2016, https://www.wired.com/2015/07/hackers-heist-semis-exploiting-satellite-flaw/; Lorenzo Franceschi-Bicchierai, "This $1,000 Device Lets Hackers Hijack Satellite Communications," *Motherboard,* July 31, 2015, https://motherboard.vice.com/en_us/article/xywjpa/this-1000-device-lets-hackers-hijack-satellite-communications.
[36] David Livingstone and Patricia Lewis, "Space, the Final Frontier for Cybersecurity?"
[37] de Wet, "Satellite networks."

been used to temporarily bring down individual websites, in addition to attacking internet service providers (ISPs) and backbone companies, causing connectivity issues worldwide.[38] The uses of DDoS attacks do not stop with the internet. A November 2016 DDoS attack in Finland disabled computers that were controlling heating in the building.[39] These types of DDoS attacks that impact connectivity and operations of physical infrastructure could potentially interfere with critical systems that control satellites or could be used to cause a wide-range blackout of information distribution.

There also exists the potential that an ideologically driven VNSA, seeking to deny the use of space for all actors, might pursue a strategy of intentionally creating space debris in order to increase the likelihood that a cascade of collisions (which would create exponential amounts of space debris) might occur. In theory, this scenario – known as the Kessler syndrome for the NASA scientist who first proposed it in 1978, Donald Kessler – could leave a "distribution of debris in orbit that could render space exploration, and even the use of satellites, unfeasible for many generations."[40] This domino scenario becomes increasingly likely as the number of space objects increases. As the pace of space innovation and production increases, so do the number of new satellites in orbit and the number of old satellites that are inoperative but remain in orbit.[41]

So far, the discussion of space-based threats has focused on how MNSAs can affect the use of space-based infrastructure by the U.S. military and civilian sectors. However, there are also significant risks associated with potential uses of space-based information systems. Of particular importance is the ability of all actors, including adversaries, to exploit satellite or radar imagery for intelligence and planning purposes. According to industry experts, by 2020 there will be enough satellites in space to capture real-time surveillance of the entire world.[42] The government does not have a monopoly on the collection or distribution of satellite imagery, which can often be commissioned by anyone with the ability to pay commercial providers. High-quality satellite images are already being used by, for example, real estate developers and city planners, to create 3D models of building sites.[43] A violent MNSA could use open source imagery such as Google Earth, or purchase satellite imagery as an operational planning tool to create models of intended targets, conduct photo reconnaissance or rehearse a course of attack. Exploiting technology for these purposes has become especially relevant as more conspicuous on-the-ground target reconnaissance is becoming more difficult due to heightened security and scrutiny of suspicious behavior.[44]

---

[38] *Wired,* "The Biggest Security Threats Coming in 2017," January 2, 2017, https://www.wired.com/2017/01/biggest-security-threats-coming-2017/.
[39] *Metropolitan.fi,* "DDoS attack halts heating in Finland amidst winter," http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter.
[40] Donald Kessler and Burton G. Cour-Palais, "Collision Frequency of Artificial Satellites: The Creation of a Debris Belt," *Journal of Geophysical Research*, 83, no.6 (1978): 2637–646, http://webpages.charter.net/dkessler/files/Collision%20Frequency.pdf; "*Kessler Syndrome",* Website,http://gravitymovie.wikia.com/wiki/Kessler_Syndrome.
[41] Steve Olson, "The Danger of Space Junk," *The Atlantic,* July 1998, https://www.theatlantic.com/magazine/archive/1998/07/the-danger-of-space-junk/306691/.
[42] Jason Murdock, "How Satellite Surveillance is Helping to Predict Stock Prices," *Newsweek,* March 2, 2017, http://www.newsweek.com/how-satellite-surveillance-helping-predict-stock-prices-skynet-562973.
[43] Qihao Weng, "Remote sensing of impervious surfaces in the urban areas: Requirements, methods, and trends." *Remote Sensing of Environment* 117 (2012): 34-49.
[44] Anthony Kimery, "Mumbai Terrorists' Use Of Google Earth Re-Ignites Concerns," *Homeland Security Today,* Decemer 5, 2008, http://www.hstoday.us/columns/global-watch/blog/mumbai-terrorists-use-of-google-earth-re-ignites-concerns/642770639e0a4ae59d34a79be3a628fa.html.

For example, MNSAs could easily exploit commercially available services such as TOPO, which allows users to print 3D topographical models of any location on earth.[45] While intended as a novelty, the 3D models are sufficiently detailed to help would-be attackers plan their use of terrain features for cover and concealment. Another cheaply available service, the SpyMeSat application allows iPhone users to purchase existing high-resolution imagery for between US$10-US$80. Users of the app can also task the EROS-B satellite operated by ImageSat International to shoot 70cm black and white photos of their desired location. New taskings can be ordered for as little as US$500.[46] Yale University's Jason Lyall was able to use a similar service to locate all Russian field artillery installations during the second Chechen war. Specifically, he used Arcview GIS (commercially available geographic information systems (GIS) software, available, for example, at any major university) to draw 30km (the maximum range of Russian 152mm 2A65 field guns) radial plots around the position of each artillery strike. He then used commercial satellite imagery to confirm suspected base locations and rule out possible alternative locations.[47] Similarly, the BBC was able to commission detailed satellite images to confirm rumors that Iran was building a permanent military base south of Damascus, Syria.[48]

Beyond being able to purchase imagery and topographical maps, firms that specialize in satellite imagery and surveillance are offering intelligence services to customers seeking "alternative data" advantages. Firms such as Orbital Insight, in partnership with private satellite operators, are combining satellite imagery with deep learning data science methods to characterize and classify images, producing valuable insights on industries ranging from agriculture to oil production. AJ DeRosa, an executive at Orbital Insights, explains "our platform can see cars, trains, planes, oil tanks, anything that you want. Once that's done, we can throw it to the data science algorithms and actually create information and insight from that. Then, we can deliver it through a web portal or an API."[49] For example, the firm was able to extract valuable information on China's oil production by creating a neural network to find tanks in satellite images. They discovered at least 2,001 storage tanks, whereas publically available documentation notes just 500. (In short, they discovered that Chinese strategic oil reserves were more than four times greater than the Chinese government indicated.) They were also able to monitor oil levels by observing the floating roofs of oil tanks and measuring their projected shadows to determine the level of oil contained within the tanks.[50] While these technological advances are leading to insights that could have tremendous positive humanitarian and economic implications, they could just as easily be exploited by adversaries to cause harm.

Consequently, national security expert John Bumgarner warned, "unrestricted access to open source imagery has the potential to be a national security threat," and while "technologies like Google Earth have enormous untapped economic potential in the global market…these same technologies also have the potential to be greatly misused in ways we cannot even dream about today."[51] Indeed, the Mumbai attackers took advantage of these technologies. They were assisted by GPS equipment when they covertly

[45] TE Halterman, "Terrain2STL Lets Users 3D Print Topographic Maps from Google Maps Data," *3DPrint.com*, July 21, 2015, https://3dprint.com/83026/terrain2stl-3d-print-maps/.
[46] Mel Martin, "SpyMeSat iOS app now lets you buy hi-resolution satellite images," *Engadget,* July 13, 2014, https://www.engadget.com/2014/06/13/spymesat-ios-app-now-lets-you-buy-hi-resolution-satellite-images/;https://www.spymesat.com/.
[47] Lyall, Jason. "Does indiscriminate violence incite insurgent attacks? Evidence from Chechnya." *Journal of Conflict Resolution* 53, no. 3 (2009): 331-362.
[48] Gordon Corera, "Iran building permanent military base in Syria – claim," *BBC News,* November 10, 2017, http://www.bbc.com/news/world-middle-east-41945189.
[49] Murdock, "How Satellite Surveillance."
[50] Ibid.
[51] Kimery, "Mumbai Terrorists' Use Of Google Earth."

infiltrated India from Pakistan. They also carried high-resolution satellite imagery that they used in planning their attack. Finally, they used satellite communications equipment.[52]

In addition, MNSAs have also proven capable of hijack satellite signals to disseminate propaganda. For example, in 2007, U.S.-based satellite communications provider, Intelsat was informed that the LTTE (Liberation Tigers of Tamil Eelam) were accessing an unused channel on one their Satellite 12 to broadcast their TV and radio propaganda: Television of Tamil Eelam and Voice of the Tigers (radio). Even after being made aware of LTTE's illegal broadcasts, Intelsat was not immediately able to shut it down.[53] A similar approach was used by the Falun Gong in 2002. However, instead of using an unused communications channel, the Falun Gong were able to take over a Chinese government-run television channel being broadcast from an AsiaSat satellite. The Falun Gong were therefore able to replace Chinese state television with their own programming.[54]

MNSA Types: Capabilities, Motivations and Partnerships

This section will provide a review of the existing literature on the known cyber capabilities and motivations of various MNSAs – such as hackers, cyber terrorists and violent extremist organizations (VEOs) – as well as important "unknown capabilities" that could have implications for the space domain**.** In this section, we focus explicitly on cyber capabilities, as a diverse array of MNSAs possess at least some offensive cyber capabilities and/or cyber-related intentions, which could potentially be used to target space-based infrastructure.

Because many MNSA groups possess malign intent but lack the capabilities needed to unilaterally utilize or damage space infrastructure for their purposes, and other groups possess these capabilities but lack intent, this section will also examine the potential for collaboration between MNSA groups to leverage or attack space infrastructure for malicious purposes. Importantly, disparate types of MNSAs may benefit from collaboration on successful attacks even if they do not share motivations or ideology. Moreover, MNSAs with high-end cyber capabilities (e.g., hackers) have been shown to have extremely fluid membership. Membership shifts have sometimes demonstrated radical departures from previously stated objectives.[55] Consequently, one should not assume that those MNSA groups with malicious intent

---

[52] Emily Wax, "Mumbai Attackers Made Sophisticated Use of Technology," *Washington Post Foreign Service,* December 3, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/12/02/AR2008120203519.html; Jeremy Kahn, "Mumbai Terrorists Relied on New Technology for Attacks," *The New York Times*, December 8, 2008, http://www.nytimes.com/2008/12/09/world/asia/09mumbai.html?mtrref=www.google.com&gwh=1A0ABEBE14584DB43045B32BD9C8D40B&gwt=pay; Noah Shachtman, "How Gadgets Helped Mumbai Attackers," *Wired,* December 1, 2008, https://www.wired.com/2008/12/the-gagdets-of/.

[53] "Sri Lankan Terrorists Hack Satellite," Impact Lab, http://www.impactlab.net/2007/04/13/sri-lankan-terrorists-hack-satellite/.

[54] "Hack a Satellite While It is in Orbit," Toolbox Tech, https://it.toolbox.com/blogs/rmorril/hack-a-satellite-while-it-is-in-orbit-041307.

[55] Nick Ismail, "Money, terrorism or nation state snooping – how understanding the real motives behind cyber attacks can help to prevent them," *Information Age,* June 30, 2017, http://www.information-age.com/understanding-motives-behind-cyber-attacks-can-help-prevent-123467078/; Nick Ismail, "Defending against cyber attacks is now just as important as the fight against terror – GCHQ," *Information Age,* October 9, 2017, http://www.information-age.com/cyber-security-threat-just-serious-terrorism-gchq-123468981/; Louise Shelley, John Picarelli, Allison Irby, Douglas M. Hart, Patricia Craig-Hart, Phil Williams, Steve Simon, Nabi Abdullaev, Bartosz Stanislawski, Laura Covill, "Methods and Motives: Exploring Links between Transnational Organized Crime & International Terrorism," A report for the U.S. Department of Justice, June 23, 2005, 5; Steven D'Alfonso, "Why Organized Crime and Terror Groups Are Converging," *Security Intelligence,* September 3, 2014, https://securityintelligence.com/why-organized-crime-and-terror-groups-are-converging/.

will be unable to obtain necessary capabilities from other MNSAs (or their previously affiliated members) even if their goals vary considerably. These dynamics are also discussed in this section.

Insofar as cyber-related threats are concerned, we must recognize that analysis of potential adversaries, their capabilities, and the space threats they might pose is complicated due to difficulties of attribution in the cyber realm. Cyber-attacks are often difficult to trace back to a specific actor or group, and groups or individuals may falsely claim responsibility for an attack to gain notoriety, attract publicity, or further their cause in some way. Attribution is further complicated by attempts by cyber attackers to disguise their involvement in a criminal act or to obscure the attack itself.[56] Even more complex is the difficulty of precisely identifying intentions, motives and interests of cyber actors given that, in the world of hacking, the smartest way to get away with a crime is to create a distraction while the real crime happens elsewhere.[57] Thus, it is important to keep in mind that the following analysis of MNSA motivations and demonstrated capabilities are based on incomplete information.

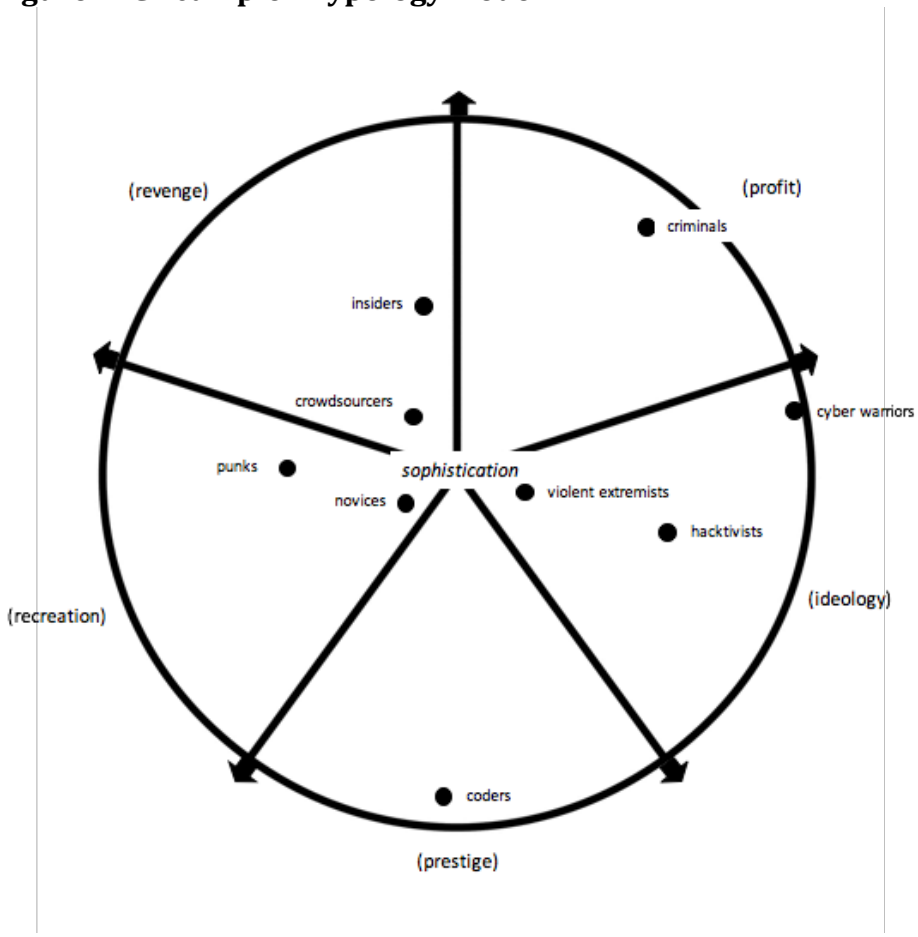
It is nevertheless possible to develop a typology of different MNSA group types. While it may not always be possible to pinpoint the precise group involved in an attack, the nature and target of an attack may still provide insights as to what type of group(s) were involved. Our group typology incorporates all existing MNSA group types that have demonstrated some sort of cyber-related activity and/or intent that could threaten space-based interests. This typology is especially important given that hacking culture differs drastically from those of government or military organizations. As such, hackers are often poorly understood, and their interests, which are likely generated by complex motivations, may not be immediately apparent or easily anticipated.[58]

Recent academic literature has attempted to disaggregate hackers based on a circumplex typology model that characterizes actors based on skill and motivation.[59] This model, depicted in figure 1 (below), is useful in capturing recent increases in ideologically and socially motivated hacking. It depicts eight types of hackers organized around five motivations and along skillset lines, to include violent extremist hackers (such as so-called jihadists) under the ideologically motivated category. This model usefully allows for a depiction of the relationship between motivations and skills. The circumplex model also allows for a depiction of relationships between hacker types (proximity as an indicator of the likelihood of a relationship) as well as a depiction of primary and secondary motivations based on where a hacker type falls relative to a near sector boundary. Consideration of the secondary motivations of each typology is useful, as most actor types are likely to possess a variety of interests that span multiple motivations that are, at times, contradictory. While some academics have proposed more complex, weighted circumplex models that use arcs and colors to depict multiple or non-adjacent motivations, the simpler model is sufficient for the purposes of this analysis.[60] Nevertheless, an important caveat is in order: many of these hackers are opportunistic and willing to affiliate with organizations (in this case, violent extremists) with which they do not share an origin story or ideology for publicity or convenience.[61]

---

[56] Phil Williams and Dighton Fiddner, *Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition* (Carlisle:Army War College-Strategic Studies Institute Carlisle United States, 2016),
580; Ismail, "Money, terrorism or nation state snooping."
[57] Ismail, "Money, terrorism or nation state snooping."
[58] David Livingstone and Patricia Lewis, "Space, the Final Frontier for Cybersecurity?"
[59] Ryan Seebruck, "A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model." *Digital Investigation* 14 (2015): 36-45.
[60] Ibid.
[61] Rose Bernard, "These are not the terrorist groups you're looking for: an assessment of the cyber capabilities of the Islamic State," *Journal of Cyber Policy*, 2:2 (2017): 255-265; D'Alfonso, "Why Organized Crime and Terror Groups Are Converging."

Figure 1: Circumplex Typology Model[62]



As regards motivations – the first level of categorization – there are five categories: ideology, recreation, profit, revenge and prestige. The ideology category encompasses political activists, or those motivated by contemporary social issues, jihadists, and nationalists driven by patriotism or state-sponsored cyberwarfare. The recreation category includes those who pursue hacking for pleasure, intellectual curiosity or the general thrill of mischief. Profit is the primary motivation for criminals. Revenge is the motivation for those seeking personal vengeance or those driven by larger social justice issues. Finally, prestige includes those seeking non-material gains. These hackers are primarily non-malicious, such as white-hat hackers.[63]

The second level of categorization is along the lines of skill level, with sophistication increasing outwards along the circle's radius. Novices have a mastery of basic techniques and are mostly motivated by curiosity. Crowdsourcers are less technically inclined and are motivated first by revenge, and secondly by recreation. Hacktivists are of lower to intermediate skill level and are driven primarily by political ideology. Insiders have mid-level skills and are motivated by revenge or profit. Punks are of low to average skill and are primarily motivated by the thrill of deviant behavior and secondly by revenge. Criminals are mostly of upper-intermediate skill and are driven primarily by profit and secondly by

[62] Nodes depict hacker types; nodes placed near to circle edges are more sophisticated; regular text indicates hacker groups; parenthesized text indicates motivations. Figure adapted from R. Seebruck/ Digital Investigation 14 (2015) 36-45.
[63] Seebruck, "A typology of hackers."

revenge. Coders are typically non-malicious hackers with upper-intermediate skills primarily seeking prestige. Cyber warriors are highly sophisticated attackers motivated by ideology and profit.[64]

Violent Extremists

Violent extremists include jihadists, terrorists and other types of violent non-state actors with ideological motivations. These types of actors generally accept or encourage the use of political violence. Typically, the level of motivation of this actor type exceeds their actual cyber capabilities (as they are mostly amateurs, as will be discussed further below), although they may share common intersections with other types of hackers that could serve to enhance their capabilities indirectly. Like other types of hackers, however, ideology is rarely the sole motivation for these actors. Moreover, sometimes, ideology may not even be the primary motivation but merely a matter of convenient affiliation.[65] Unlike other cyber actors who are more likely to want to obscure their involvement in the cyber domain, this type of actor welcomes the attention. They are likely to want to take credit for successful attacks to attract attention to their cause and bolster its legitimacy.

For the most part, these types of hackers have very low skill levels and usually use pre-written hacking scripts known as "toolkits."[66] However, violent extremists might have a special interest in acquiring the skills and capabilities necessary to execute damaging cyber-attacks.[67] Former FBI Director James Comey warned of cyberattacks by terrorists at the 2015 Cybersecurity Law Institute at Georgetown University, stating, "destructive malware is a bomb. Terrorists want bombs." Regarding the utility of using digital weapons to strike the United States from afar, as opposed to infiltrating terrorists across the border, Comey said, "I see them already starting to explore things that are concerning, critical infrastructure, things like that. The logic of it tells me it's coming, and so of course I'm worried about it."[68] Of all MNSA types, violent extremists are most likely to want to cause destruction and highly visible chaos, such as initiating a Kessler-style cascade of collisions, in order to attract publicity and further their cause. Violent extremists that espouse archaic worldviews (such as the Islamic State of Iraq and the Levant (ISIL) and, to a lesser extent, al-Qa'ida) may find it appealing to deny the use of space as a domain for technological innovation and modern infrastructure. Importantly, this type of actor is also the most likely to want to exploit space-based information systems and infrastructure to conduct or enable other types of violent attacks on the ground.

Al-Qa'ida

Of the violent extremist organizations considered in this report, al-Qa'ida has demonstrated the most interest in cyber warfare, at least in terms of official rhetoric. Al-Qa'ida's interest in cyber jihad can be traced back as far as the mid-1980s. One of Osama bin Laden's mentors, Sheikh Abdullah Azzam, a Palestinian Sunni Islamist cleric who convinced bin Laden to join the jihad in Afghanistan, encouraged jihadis to exploit the potential of evolving technologies. The evolution of al-Qa'ida's philosophy has incorporated the internet in a variety of ways including training, planning, logistics and the establishment

[64] Ibid.
[65] Bernard, "These are not the terrorist groups you're looking for."
[66] C.A. Meyers, S. S. Powers, and D. M. Faissol, *Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches*. No. LLNL-TR-419041. Lawrence Livermore National Laboratory (LLNL), Livermore, CA, 2009, https://e-reports-ext.llnl.gov/pdf/379498.pdf.
[67] John Rollins and Clay Wilson, "Terrorist capabilities for cyberattack: Overview and Policy issues." Congressional Research Service Report to Congress, (2006), https://fas.org/sgp/crs/terror/RL33123.pdf.
[68] Joseph Marks, "ISIL aims to launch cyberattacks on U.S.," *Politico,* December 29, 2015, http://www.politico.com/story/2015/12/isil-terrorism-cyber-attacks-217179.

of cyberspace as a legitimate field of battle.[69] The importance of cyber-jihad has been discussed in detail by al-Qa'ida's leadership, including bin Laden and Zawahiri, as well as al-Qa'ida in the Arabian Peninsula and al-Qa'ida in the Islamic Magreb leadership. In his 2008 book, Abd al-Bari 'Atwan, a pro-jihad author who interviewed bin Laden in 1996, wrote a chapter titled "Cyber Jihad" emphasizing the importance of cyberspace as a front for battle.[70] Al-Qa'ida explicitly confirmed its interest in the internet in a 2012 video calling for "electronic jihad" where the narrator notes "Internet piracy is an important field of jihad," and encourages followers with expertise to "target the websites and information systems of big companies and government agencies of the countries that attack Muslims."[71] It also called for cyber-attacks against networks such as the electric grid and compared vulnerabilities to U.S. critical cyber networks to vulnerabilities in the aviation system before 9/11.[72] Importantly, this video serves as a justification for the use of modern technologies and cyberspace as a field of battle, as some elements of this kind of struggle are philosophically inconsistent with some of al-Qa'ida's principles. Al-Qa'ida's interest in cyber-attack is in part a result of its dispersion and move underground post 9/11.[73] Cyber war is an effective way to shift conflict into a different domain where dispersion is an asset rather than a (potential) weakness.

In terms of what we know about al-Qa'ida's cyber capabilities, it has not demonstrated a high level of sophistication. Despite claims that it is building a cyber-unit, it has not successfully launched any significantly damaging attacks, indicating that they are probably novices. However, heavily redacted court documents from the case of a man accused of being one of al-Qa'ida's top recruiters is evidence that the group may have launched successful offensive cyber-attacks, including one against government computers in Israel. These attacks were, however, relatively unsophisticated and occurred before November 2001, when the suspect was arrested.[74] Nevertheless, Abd al-Bari 'Atwan's book quotes a "senior former intelligence source" who claimed that al-Qa'ida recruited highly skilled computer experts, such as computer professors from Eastern Bloc countries to hack against Western targets including systems controlling airports and power and water supplies. However, it does not appear that these attacks too place. [75]

There is also evidence that they are cooperating with other criminal organizations (at least for financial gain and smuggling purposes; see below discussion on cross-group cooperation).[76] Post-9/11 crackdowns have impinged on al-Qa'ida's financial flows, forcing it to employ innovative approaches to financing.[77] Experts believe that al-Qa'ida has turned to organized crime groups for money laundering expertise, in addition to trying to recruit experts in the relevant technologies to help overcome money supply issues. Russian cyber-crime expert Dr. Mark Galeotti explains how, "on the whole they [al-Qa'ida]

---

[69] Steven Stalinsky and R. Sosnow, "From Al-Qaeda To The Islamic State (ISIS), Jihadi Groups Engage in Cyber Jihad: Beginning With 1980s Promotion Of Use Of 'Electronic Technologies' Up To Today's Embrace Of Social Media To Attract A New Jihadi Generation," *The Middle East Media Research Institute,* (IOS Press Ebooks, 2014) 86.
[70] Ibid.
[71] CNN Wire Staff, "U.S. Senators: Al Qaeda calls for 'electronic jihad'," *CNN,* May 23, 2012, http://www.cnn.com/2012/05/23/politics/al-qaeda-electronic-jihad/index.html.
[72] Ibid.; Jack Cloherty, "Virtual Terrorism: Al Qaeda Video calls for 'electronic jihad'," *ABC News,* May 22, 2012, http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875.
[73] Peter Warren, *Cyber Alert: How the World is Under Attack from a New Form of Crime (*Vision, 2005), 114.
[74] Alex Kingsbury, "Documents Reveal Al Qaeda Cyberattacks," *U.S. News,* April 14, 2010, https://www.usnews.com/news/articles/2010/04/14/documents-reveal-al-qaeda-cyberattacks.
[75] John Chariton "Al Qaeda buys cyber criminal expertise." *Computer Fraud & Security* 2005, no. 3 (2005): 2.
[76] Terry Carter, "Organized crime leaders and terrorists cross paths in cyberspace," *ABA Journal,* January 2014, http://www.abajournal.com/magazine/article/organized_crime_leaders_and_terrorists_cross_paths_in_cyberspace.
[77] Chariton "Al Qaeda buys cyber criminal expertise."

are looking to buy expertise rather than depend on people they have indoctrinated because it is easier and quicker and there are less links. Al-Qa'ida Qa'idais paying three times what Russian organized crime is charging the Cosa Nostra."[78] In sum, while it does not appear that al-Qa'ida has successfully perpetrated any damaging cyber-attacks, it would like to. This may be achieved through partnerships with other, more capable MNSAs.

Concerning the use of satellite imagery, there is evidence that al-Qa'ida has used space-based intelligence garnered from satellite images to plan and execute violent attacks in Iraq and Yemen. In July 2016, footage was obtained showing Google Earth being used as a tactical planning tool against military targets in Iraq, according to an OSC report, which also revealed that in September 2006, al-Qa'ida-linked militants in Yemen exploded four car bombs in a failed attack on oil facilities, planned with the aid of Google Earth. An al-Qa'idatraining manual stated that by "using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about the enemy."[79] Furthermore, during raids on al-Qa'ida safe houses in Afghanistan, laptops were found with the schematics of U.S. critical infrastructure obtained by mining online GIS data and other resources. Terrorists' laptops have also been found to contain considerable data on North American oil and gas pipelines and infrastructure. According to military intelligence officials, al-Qa'ida has also used Google Earth imagery to plan and carry out attacks in Iraq. For example, Google Earth images of British military were discovered in the homes of Iraqi insurgents. After a planned attack targeting multiple U.S. cities was thwarted by coalition forces in Iraq, Google Earth imagery of potential targets was found, as well as information indicating that the plot had received approval from al-Qa'ida's leadership. Moreover, in December 2006, al-Qa'ida penetrated a protected military zone in Algiers and bombed a bus of foreigners working on a U.S. based KBR oil project. Following the attack, the al-Qa'ida faction responsible posted a video of the assault footage and details of how it was planned using satellite imagery from Google Earth, which allowed attackers to familiarize themselves with the bus route and ground features. This use of satellite information systems is likely to continue as open source and commercial satellite images and surveillance become even more ubiquitous in the private sector.[80]

ISIL

ISIL's motivations and intentions in the cyber realm are somewhat murky and complicated by the fact that the brand has become a banner under which unsanctioned offshoots and lone actors operate unofficially. While the organization is famous for its use of digital technologies as strategic tools for recruitment, communication and logistical planning, ISIL has not demonstrated significant intent or capability to wage cyber warfare. Rose Bernard explains, "the omnipresence and professionalization of internet use by IS[IL] supporters have led to a conflation of their presence online with a capability to undertake cyber-attacks…however official IS[IL] cyber capability is overwhelmingly focused on their own operational security and resilience"[81]

Despite demonstrated mastery of the internet as a tool for organizational growth, there are significant philosophical contradictions that complicate cyber (or space) as a strategic domain for attack. ISIL's worldview rejects modern technologies even more so than al-Qa'ida's, though it has likewise justified the permissibility of using modern technology for cyber warfare. For example, discussions on Al Khelafa Europe, a popular pro-ISIL online forum, agreed that ISIL needed to investigate cyber-attacks targeting

[78] Ibid.
[79] Kimery, "Mumbai Terrorists' Use Of Google Earth Re-Ignites Concerns."
[80] Ibid.
[81] Bernard, "These are not the terrorist groups you're looking for," 256.

manned and unmanned military aircraft. This indicates that while ISIL and supporters recognize that cyber can be used for destructive purposes, ambitions do not extend beyond the battlefield.[82] However, as ISIL is forced to retreat into insurgency and disperse, just as al-Qa'ida did, the current prioritization of battlefield cyber capabilities over broader cyber warfare activities might not last.[83]

ISIL does not officially recognize any pro-ISIL cyber group, nor does it have any official group responsible for the coordination and implementation of destructive cyber-attacks. As such, ISIL's online presence can be broken down into two different identities, an official "Islamic State online" – consisting of officials news outlets, spokespersons, etc. – and pro-ISIL online groups which have declared allegiance to ISIL but which are not necessarily affiliated and therefore do not take direction from the official center.[84] The latter type includes the informal networks of cyber activist groups that have pledged allegiance to ISIL. Such groups include the Islamic State Hacking Division, United Cyber Caliphate (UCC), United Islamic Cyber Force, Cyber Khalifah, Cyber Caliphate Army (CCA) and Islamic Cyber Army. These groups all claim to be official ISIL hackers, despite the fact that ISIL has sought to explicitly disassociate itself from them.[85] Investigations into some of these groups demonstrates inconsistencies between their other affiliations and the ISIL worldview. This indicates that hacking groups are likely to be motivated by more than an avowal of a particular ideology and that relationships are fluid.[86]

While ISIL may not possess the skills needed to execute a damaging attack at present, this does not mean that they will not pose a threat in the future. According to Laith Alkhouri the threat is high "because they are utilizing multiple ways of attracting new talent, utilizing all the freely available tools online, utilizing malware that is already available and building their own malware."[87] As other groups share their success online, that information will become available to hackers of all stripes, ISIL included. Ultimately, the intention to build/purchase technology such as jammers to gain kinetic/battlefield advantages has been unofficially stated, and is probably within the realm of possibility for ISIL if given the appropriate opportunities for technology transfer and cooperation with more technologically sophisticated organizations. More complex cyber-attacks targeting space-based systems are likely outside of ISIL's capacity. This does not however preclude ISIL collaborating with a more capable cyber partner to purse these types of attacks.

Lashkar-e-Taiba

Lashkar-e-Taiba, a Pakistani Wahhabi group established in 1987, warrants special mention as a VEO that has used space-based systems in the past and has the potential to pose serious cyber and space threats in the future. The group has a steady supply of volunteers, funding and concerted state support.[88] It is one of the most technically sophisticated terrorist groups in existence, as demonstrated by its execution of the 2008 Mumbai attacks. It has focused mainly on using its cyber expertise to safeguard its communications.[89] It recruits from top Pakistani universities and often pays more than local tech companies, giving the group its pick of talent. It was founded by engineering instructors at a university in

[82] Bernard, "These are not the terrorist groups you're looking for," 258.
[83] Marks, "ISIL aims to launch cyberattacks on U.S."
[84] Bernard, "These are not the terrorist groups you're looking for," 256.
[85] ISIL Telegram, 6 July 2016.
[86] Bernard, "These are not the terrorist groups you're looking for," 259.
[87] Alkhouri, Kassirer and Nixon, "Hacking for ISIS."
[88] V.S. Subrahmanian, Aaron Mannes, Amy Sliva, Jana Shakarian, and John P. Dickerson. "A Brief History of LeT." In *Computational Analysis of Terrorist Groups: Lashkar-e-Taiba*, (New York: Springer, 2013), pp. 23-68.
[89] Marks, "ISIL aims to launch cyberattacks on U.S."

Lahore, Pakistan, where it retains ties to major political parties and the Pakistani military.[90] While it has not yet perpetrated offensive cyber-attacks, there is a distinct possibility that the group possesses the requisite skills and knowledge necessary to execute a damaging attack either on their own or in collaboration with other VEOs. As previously noted, the group relied heavily on open-source images from Google Earth to plan and execute the 2008 Mumbai attack. They were able to conduct rehearsals using high-resolution satellite maps and conduct reconnaissance on the area remotely without setting foot on the ground. Although they were not sailors, they were able to approach the city by boat using GPS navigation.[91] They also used Thuraya satellite phones and Voice over IP technology to communicate with their counterparts in Karachi who were monitoring events on TV and relaying intelligence to the attackers in real-time.[92]

Criminals

Criminal hackers include individual hackers working alone, as part of organized gangs, mafias or transnational criminal organizations, or as state-sponsored hackers. Criminals are mostly of upper-intermediate skill and are driven primarily by profit and secondarily by revenge.[93] Like with other types of hackers, alliances and networks between these actors are fluid and change constantly depending on opportunity and advantage. For example, these types of criminals are interested in grand operations such as currency manipulation on a massive scale.[94] These types of hackers may also be "guns for hire" and are often employed by organized crime and by VEOs, as previously mentioned.[95]

Unlike traditional crime, cyber-crime has the advantages of being able to quickly target vast numbers of victims without requiring physical proximity of the attacker to the target.[96] Attribution in this category is particularly difficult as cyber criminals attempt to obscure their criminal activity so that they can avoid detection and continue to exploit and profit from security breaches.[97] Criminal elements have demonstrated proficiency in building complex systems designed to steal money and intellectual property at a grand scale. It is estimated that online criminal activity costs the global economy as much as counterfeiting or narcotics at over $400 billion per year.[98]

As discussed in the previous section on space vulnerabilities, these types of criminals are capable of executing spoofing attacks on the communications networks of financial institutions such as banks and stock exchanges, or might exploit automatic time stamp and other functions for fraudulent purposes.

Cyber Warriors

Cyber warriors are highly sophisticated attackers motivated primarily by ideology and secondarily by profit. These actors include those motivated by political ideology, nationalism or religion.[99] Typically, they seek to conduct attacks that destabilize, disrupt or destroy the cyber assets and data of an enemy

[90] Subrahmanian et al. *Computational Analysis of terrorist groups: Lashkar-e-Taiba*.
[91] Kimery, "Mumbai Terrorists' Use Of Google Earth Re-Ignites Concerns."
[92] Subrahmanian et al. *Computational Analysis of terrorist groups: Lashkar-e-Taiba*.
[93] Seebruck, "A typology of hackers."
[94] Ismail, "Money, terrorism or nation state snooping."
[95] Kim-Kwang Raymond Choo and Russell G. Smith. "Criminal exploitation of online systems by organised crime groups." *Asian journal of criminology* 3, no. 1 (2008): 37-59.
[96] Meyers, Powers, and Faissol, *Taxonomies of cyber adversaries and attack, 3.*
[97] David Livingstone and Patricia Lewis, "Space, the Final Frontier for Cybersecurity?"
[98] Steve Ranger, "Organised cybercrime groups are now as powerful as nations," *ZDNet,* June 9, 2014, http://www.zdnet.com/article/organised-cybercrime-groups-are-now-as-powerful-as-nations/.
[99] Seebruck, "A typology of hackers."

nation or organization.[100] Cyber warriors include groups backed by states that want to engage in cyber warfare against the United States and other countries that possess militaries that are superior in other, more conventional domains. Shifting an asymmetric conflict to the cyber domain might balance or tip the scales in favor of an otherwise weaker adversary. Thus, cyber warriors are highly coveted by states seeking to compete with the United States and other militarily superior nations. This type of hacker is the most sophisticated and dangerous, especially given the access and resources afforded by the backing of a state actor.

Cyber warriors are often recruited online. For example, Russian government recruiters have scouted programmers by placing ads on social media sites, offering lucrative employment to students and professional coders, and tapping into Russian organized crime networks for potential talent. According to intelligence reports, such recruits were intended to cycle through military contracting companies and newly formed units called science squadrons established on military bases around the country.[101] Sometimes, the incentive to participate in government-sponsored hacking is simply to avoid negative repercussions. For example, Russia's massive cyber-crime underworld is filled with what it describes as "hackers who have problems with the law,"[102] who would rather work on behalf of the state than go to prison. Furthermore, those subject to mandatory conscription might consider hacking a preferable alternative to serving in more dangerous fields, with the added benefit of being more profitable than other forms of services.[103] These recruits might not be loyal to the ideologies of the state but are developing skills and making connections in the process of hacking on its behalf. They might be persuaded in a variety of other directions for other causes, including for-profit criminal endeavors, hacking on behalf of VEOs, etc.

Cyber warriors are employed to conduct cyber warfare, including espionage, on behalf of the state. In Estonia in 2007, following the removal of a Russian WWII monument, there was a massive DDoS attack that shut down the websites of Parliament, several national newspapers and Estonia's central bank.[104] Investigation by national security agencies have determined that hackers paid by the Russian government breached the Democratic National Committee and the Democratic Congressional Campaign Committee.[105] The perception that these attacks succeeded in influencing the 2016 presidential election could embolden the sponsors of cyber warriors to try new targets and techniques such as data sabotage or attacks on physical infrastructure.[106]

A report by the US-China Economic and Security Commission includes the claim that in October 2007 and July 2008 hackers interfered with the connection from a ground station to affect the operation of the

---

[100] Laith Alkhouri, Alex Kassirer and Allison Nixon, "Hacking for ISIS: The Emergent Cyber Threat Landscape," Flashpoint Report, April 2018.
[101] Andrew Kramer, "How Russia Recruited Elite Hackers for Its Cyberwar," *The New York Ties,* December 29, 2016, https://www.nytimes.com/2016/12/29/world/europe/how-russia-recruited-elite-hackers-for-its-cyberwar.html.
[102] Ibid.
[103] Ibid.
[104] Ellen Nakashima and Jack Gillum, "Russian government hackers used antivirus software to steal U.S. cyber capabilities," *The Washington Post,* October 5, 2007, https://www.washingtonpost.com/world/national-security/russian-government-hackers-exploited-antivirus-software-to-steal-us-cyber-capabilities/2017/10/05/a01bf546-a9fc-11e7-92d1-58c702d2d975_story.html?utm_term=.4f099ea41aa8.
[105] Lily Hay Newman, "Hacker Lexicon: What is the Attribution Problem," *Wired,* December 24, 2016, https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/; Eric Lipton, David E. Sanger and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," December 13, 2016, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.
[106] *Wired,* "The Biggest Security Threats Coming in 2017."

Landsat 7 and Terra (EOS AM-1) satellites, which are used for earth observation. The Landsat 7 satellite experienced 12 minutes of interference in October 2007, followed by the Terra experiencing two minutes of interference in June 2008. In July 2008, the Landsat 7 experienced another 12 minutes of interference, and in October 2008 the Terra was affected by interference for nine minutes.[107] The commission is concerned that the hack was perpetrated by Chinese government-sponsored hackers, to assess the vulnerability of the satellite control systems.[108] The hacks are believed to have been carried out via a commercial satellite station in Norway used by NASA for data transfers over the internet. The mission operation center is capable of sending data including orbit and maneuvers. As such, the hackers could potentially send false data to cause a satellite to enter the atmosphere in an uncontrolled way, which could cause it to burn up, possibly resulting in large pieces landing on earth at unpredictable locations.

The demonstrated capabilities of hackers backed by the resources of state adversaries make it exceedingly likely that state proxies would have the most potential to interfere in space, especially if the state was a major player in the space domain with military or commercial technology production. This is potentially the case even without the consent of the groups' state benefactors.

Hacktivists

Hacktivism is a broad category of cyber activity and is the domain of ideologically motivated underground organizations and individuals unhappy about a perceived injustice.[109] However, even within single organizations, they are not as cohesive in purpose and ideology as previously believed. While hacktivists are primarily motivated by ideology, secondary motivations include recreation, prestige or revenge and vary across individuals and groups. Hacktivists are politically or socially motivated, combining activism and hacking to champion their causes and present themselves as vigilantes. Unlike cyber warriors, they are not state-sponsored, and governments are often the targets for hacktivist attacks. The concept of government tends to be anathema to many hacktivists, who tend to be anti-establishment and subscribe to extremely libertarian views. They place supreme importance on internet freedom and freedom of speech.[110] Hacktivists are typically of lower to intermediate skill level, although some have advanced skills.[111]

One of the most notorious hacking groups is Anonymous, a loosely connected, leaderless movement of hackers and offshoots. On its website, it describes itself as a "relatively small vigilante cyber group" that has "expanded and transformed into a continuation of the Civil-Rights movement."[112] While Anonymous rose to prominence as defenders of open internet and freedom of speech, some of its offshoots such as LulzSec and AntiSec, have adopted more recreational ideologies.[113] In response, new offshoots have emerged, such as MalSec, that espouse more altruistic goals such as exposing online security weaknesses

[107] Charles Arthur, "Chinese Hackers Suspected of Interfering with US Satellites," *The Guardian,* October 27, 2011 https://www.theguardian.com/technology/2011/oct/27/chinese-hacking-us-satellites-suspected; Jim Wolf, "China Key suspect in U.S. satellite hacks: commission," *Reuters,* October 28, 2011, china-usa-satellite-idUSN1E79R1LK20111028; Daniel Livingstone, 'The Intersection of Space and Cybersecurity is a Growing Concern', Chatham House Expert Comment, November 25, 2014.
[108] "2011 Report to Congress of the U.S.-China Economic and Security Review Commission," One Hundred and Twelfth Congress, November 2011, https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf.
[109] Seebruck, "A typology of hackers."
[110] Saadawi and Colwell, Jr. *Cyber infrastructure Protection Volume III*, 157.
[111] Seebruck, "A typology of hackers."
[112] Ibid.
[113] William Pendergrass, *What is anonymous?: a case study of an information systems hacker activist collective movement.* (Ann *Swing Time* (New York: Penguin Press, 2016), 315–16.

without compromising civilian information or capital.[114] This divergence in ideology demonstrates the difficulty of anticipating cyber threats based on actor type alone.

A recent article concluded that, "hacktivism…is likely to become an increasingly common method for voicing dissent and taking direct action against adversaries. It offers an easy and inexpensive means to make a statement and inflict harm without seriously risking prosecution under domestic criminal law or a response under international law. Hacking gives non-state actors an attractive alternative to street protests."[115]

While drug dealers, pedophiles, corporations, and other entities deemed to be corrupt or harmful to the common good are often targeted by hacktivists, so too are governments.[116] Hacktivists have successfully frozen government servers, defaced websites, and hacked into data or email and released it online. Hacktivists typically launch DDoS attacks, spreading malware that infects routers and DVRs and coordinates them to overwhelm an online target with a glut of internet traffic.[117] However, they often have other objectives such as obtaining and releasing data that is damaging to the target in some way, such as exposing corruption.[118] For example, the release of the Panama Papers, which exposed influential individuals who were hiding money in offshore accounts, was done with the express purpose of exposing the extent of financial corruption.[119]

While hacktivists profess to be defenders of justice, this is not always demonstrated to be the case. For example, big attacks by hacktivists over the last couple of years against the National Health Services and Parliament in the United Kingdom (e.g. WannaCry, NotPetya) have been identified by the Government Communications Headquarters (GCHQ) as just as important, if not more important than fighting international terrorism.[120] Hacktivists have compromised sensitive information on civilians in the process of furthering their causes, and have damaged trust in digital information systems and their security.[121] As space becomes more heavily integrated into global infrastructures, hacktivists will inevitably find it attractive to hack satellite communications for similar purposes, such as exposing questionable financial transactions – especially now that a lot of financial service providers are shifting to relying on more space-based infrastructure.

Cooperation

Cooperation between non-state actors not only involves working together to pursue mutually beneficial outcomes, but often involves the transfer of technology or knowledge from one organization to another. Hackers frequently share their success, or important lessons from failed operations, on the internet. This exponentially increases global vulnerability to future hacking attempts by all types of hackers, regardless

[114] Samantha Murphy, "New hacktivist sect emerges from anonymous," *New Scientist,* April 18, 2012, https://www.sciencedirect.com/science/article/pii/S0262407912610070?via%3Dihub.
[115] Dorothy Denning, "The Rise of Hacktivism," *Georgetown Journal of International Affairs,* 2015.
[116] Jenni Bergal, "Hacktivists launch more cyberattacks against local, state governments," *PBS News Hour,* January 10, 2017, https://www.pbs.org/newshour/nation/hacktivists-launch-cyberattacks-local-state-governments.
[117] Elinor Mills, "Old-time hacktivists: Anonymous, you've crossed the line," *CNet,* March 30, 2012, https://www.cnet.com/news/old-time-hacktivists-anonymous-youve-crossed-the-line/.
[118] Dan Lohrman, "Understanding New Hacktivism: Where Next for Hackers With a Cause" *Government Technology,* July 31, 2016, http://www.govtech.com/blogs/lohrmann-on-cybersecurity/understanding-new-hacktivism-where-next-for-hackers-with-a-cause.html.
[119] Ibid.
[120] *Wired,* "The Biggest Security Threats Coming in 2017."
[121] Jenni Bergal, "Hacktivists Increasingly Target Local and State Government Computers," *Huffington Post,* January 11, 2017, https://www.huffingtonpost.com/entry/hacktivists-increasingly-target-local-and-state government_us_587651e8e4b0f8a725448401.

of affiliation or motivation. For example, the well-known hacker database, Shodan, provides advice on how to best exploit everything from power plants to wind turbines.[122] Providers of such information on Shodan (or similar repositories) have no way of controlling by whom and how it will be used.

While a disaggregation of hackers is useful for threat analysis, it is important to bear in mind that the nature of the hacking universe makes developments by any type of hacker available to other types of hackers regardless of motivations or affiliations. Once a source code is made available on the internet (which is often the case), it can be used by anyone possessing the skills or knowledge necessary to execute it. Thus, the real danger of hacking generally speaking is that innovation (and potential damage) increases exponentially with every new development.[123] The ability of cyber weapons to cause catastrophic damage has already been demonstrated, and while previous attacks have revealed existing vulnerabilities, there are still many that are unknown. Furthermore, just because vulnerabilities have been identified, such as poorly secured IoT devices, does not mean that they have been successfully addressed. For example, the Mirai attack used a new weapon called the Mirai botnet that took control of poorly secured IoT devices to execute a large-scale DDoS attack, which paralyzed much of the internet in the United States on October 21,2016. The source code was released online, which sparked dozens of copycat attack armies.[124] David Fidler, a senior fellow for cybersecurity at the Council on Foreign Relations, said, "we have a serious problem with the cyber insecurity of IoT devices and no real strategy to combat it, the IoT insecurity problem was exploited on this significant scale by a non-state group, according to initial reports from government agencies and other experts about who or what was responsible. Imagine what a well-resourced state actor could do with insecure IOT devices."[125] Thus, it stands to reason that the same problems would be posed by cyber weapons that target elements of space-based infrastructure. Not only could they be used by an MNSA in an attack on a particular segment for a particular purpose, but they might be made available to other actors who can modify and expand such weapons for any number of purposes, including states with the resources to intensely develop these weapons.

A recent START publication on terrorist technology transfer has advanced on previous literature by detailing the process by which terrorists share technology and skills within and across organizations. It explains that, "cooperation and technology transfer between terrorists and other actors is far from new, and there are some well-established historical case studies that illustrate this phenomenon...comprehensive understanding of the processes by which terrorists and other VNSAs become aware of, pursue and ultimately acquire new technologies is thus fast becoming vital to anticipating and countering non-state threats. While some past and recent studies have explored the decision-making and potential for success surrounding the internal adoption by terrorists of new technologies, one essential aspect that has received relatively little prior attention has been the conditions surrounding the transfer of dangerous technologies to terrorists from a variety of outside actors."[126]

---

[122] Marc Goodman, *Future Crimes: Everything is Connected, Everyone is Vulnerable and What We Can Do About It,* New York: Doubleday, 2015; Emma Graham-Harrison, "Could Isis's 'cyber caliphate' unleash a deadly attack on key targets?," *The Guardian,* April 12, 2015, https://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race.

[123] Mark Goodman, *Everything is Connected.*

[124] "Who is Anna-Senpai, the Mirai Worm Author?" Krebs on Security, January 2017, https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/.

[125] Nicky Woolf, "DDoS attack that disrupted internet was largest of its kind in history, experts say," *The Guardian,* October 26, 2016.

[126] Rebecca Earnhardt; Gary Ackerman; James Halverson; Helena Craig and Steve Hoodjer, "Terrorist Technology Transfer," Final Report, College Park, MD: START, 2017.

Motivations for transferors and terrorists to seek and transfer include:

- Developing advantageous alliances
- Building organizational credentials and maintaining relevancy
- Shared ideology
- Increased operational success
- Uncertainty over other options
- Target audience or constituency signals desire for new technology
- Permissive environment
- Access to state sponsors[127]

While these motivations have typically involved the transfer of kinetic technologies, the same logic also applies to the transference of cyber capabilities or skills between organizations of similar or different types. For example, state sponsors of terrorism might further enable violent extremists by providing the technology and resources necessary to carry out their objectives while furthering the cause of the state. Cyber warfare in the space domain might become, for example, an extension of the competition between Iran and Saudi Arabia, which is already defined by competition using proxy actors.

More direct cooperation between MNSAs such as organized criminal groups and violent extremists can also be analyzed from a "methods, not motives" perspective.[128] While organized criminal groups are driven primarily by profit and violent extremists are motivated by ideology, nevertheless synergistic relationships are possible. Each group looks to the other for lessons learned and strategy development. Each type of group possesses specialized capabilities, and can sell or trade on those capabilities. Cooperation between Hezbollah and Mexican drug cartels exemplifies this type of exchange. Cartel tunnels have advanced significantly in terms of engineering and technology. This innovation is motivated by the profitability of the drug trade. Nevertheless, Hezbollah collaborated with the cartels and near-identical techniques have since been adopted in the design and construction of their vast networks of tunnels in Lebanon, which provide protection from Israeli airstrikes. Similarly, the Tri-Border Area of South America is home to the largest underground economy in the Western Hemisphere. Hezbollah has built relationships with transnational organized criminal groups operating in the area in order to expand their activities into this area as a means of fundraising. This provides the group an estimated $12 billion a year in illegal rents.[129]

Moreover, the aforementioned example of al-Qa'ida commissioning expertise from Russian organized criminal elements to raise funds is a prime example of how technology transfer extends into the cyber realm. Similarly, there is evidence that the Italian Mafia has worked with al-Qa'ida, drug trafficking organizations and criminal motorcycle gangs in the United States to finance terrorism, launder money and smuggle human beings. Strikingly, these groups have diverging interests, motivations and ideologies but are nonetheless willing to collaborate to capitalize on each other's unique skills or assets.[130] Furthermore, there is precedent for using cyber robbery to fund real-world attacks, as Lashkar-e-Taiba

[127] Rebecca Earnhardt, Gary Ackerman, James Halverson, Helena Craig and Steve Hoodjer, "Terrorist Technology Transfer.".
[128] Louise Shelley and John T. Picarelli. "Methods and motives: Exploring links between transnational organized crime and international terrorism." *Trends in Organized Crime*9, no. 2 (2005): 52.
[129] Alfonso, "Why Organized Crime and Terror Groups are Converging."
[130] Jennifer Hesterman, *The Terrorist Criminal Nexus: An Alliance of International Drug Cartels, Organized Crime, and Terror Groups* (Boca Raton: CRC Press, 2013).

received $2 million from hacking groups in the Philippines to help fund the 2008 Mumbai attacks. [131] Such examples shed light on the increasing convergence of criminal elements and violent extremist organizations for the transfer of technologies and skillsets.

Further evidence suggests that violent extremists in the Middle East and South Asia are increasingly collaborating with cybercriminals in Western Europe and the Americas for international money laundering, arms smuggling and drug trafficking.[132] Drug traffickers, unlike terrorist groups, are skilled in cyber messaging and encryption, and have the financial resources to attract highly skilled computer programmers. Violent extremists, who are comparatively deficient in cyber skill, often engage in illicit activities such as drug trafficking and arms smuggling for financing and as a means to weaken their Western enemies. Such links are at least indicative of violent extremists' desire to refine their cyber capabilities, as collaborative drug trafficking efforts, for example, provide them with access to pools of highly skilled computer programmers, which help enable them to operate transnationally while remaining underground and avoiding detection.[133] On the other hand, drug traffickers profit by gaining access to broader networks, markets and avenues by which to conduct illicit activity.

Links between these types of organizations indicate that violent extremists' seek to continue to refine computer skills and recruit the expertise of highly skilled computer programmers for a variety of purposes.[134] As discussed above, there is a large crossover between current pro-ISIL groups and affiliates of the Anonymous collective in South America, indicating that hacking cooperation may transcend the divergent motivations of different actors. Furthermore, previous assessments regarding the membership of hacking collectives have revealed longstanding links between Latin American and Middle Eastern hacking groups, such as those who worked to facilitate the Arab Spring, revealing that shared ideology, even in different contexts, may be as much a driver for cooperation as a single shared cause.[135]

Threat Resiliency

As space continues to evolve even more quickly over the next few years, the U.S. needs to be forward thinking about what kinds of policies and technologies will increase space resiliencies to current and future threats. Space technologies are built with an international supply chain, and as innovation and commercialization increase, it will become even harder for governments to regulate the space domain. The number of space actors is increasing with over 80 countries conducting space activities and more expected in the near future. Increasing private sector entries are lowering the cost of technology. As technology becomes more available and affordable, space innovation will become ubiquitous.[136] Any policy that seeks to secure the space domain must involve the cooperation of international actors and the private sector. Admittedly, there are significant limitations in what can be achieved with respect to international regulation and enforcement. Even if international agreements are reached among willing

[131] Emma Graham-Harrison, "Could Isis's 'cyber caliphate' unleash a deadly attack on key targets?," *The Guardian,* April 12, 2015, https://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race.
[132] Rand Beers and Francis X. Taylor, U.S. State Department, "Narco-Terror: The Worldwide Connection Between Drugs and Terror," testimony before the U.S. Senate Judiciary Committee, Subcommittee on Technology, Terrorism, and Government Information, March13, 2002; Glenn Curtis and Tara Karacan, "The Nexus Among Terrorists, Narcotics Traffickers, Weapons Proliferators, and Organized Crime Networks in Western Europe," A study prepared by the Federal Research Division, Library of Congress, December 2002, 22, [http://www.loc.gov/rr/frd/pdf-files/WestEurope_NEXUS.pdf.
[133] Rollins and Wilson. "Terrorist capabilities for cyberattack."
[134] Ibid.
[135] Bernard, "These are not the terrorist groups you're looking for," 259.
[136] Director of National Intelligence James Clapper, "Worldwide Threat Assessment of the US Intelligence Community."

parties with mutual interest in securing the space domain, there will inevitably be adversaries that will seek to find and exploit vulnerabilities that are not bound by the terms of such agreements.

In order to minimize threats, commercial satellite service providers should be incentivized to re-engineer the outdated and insecure networks upon which their technologies rely. An industry standard should also be established for new technology developers to meet. Requiring both the distributor and end users of afflicted technologies to take corrective action as soon as vulnerabilities in space-based systems emerge may also be warranted. While this would be hard to enforce, and may disrupt large swaths of industry, the alternative of critical infrastructure becoming even more embedded in buggy and archaic systems entails far more serious consequences. A final option is to try to limit the technology transfer of dangerous cyber skills or technologies by further cracking down on organized criminal elements with the express intent of disrupting the nexuses between different types of MNSA actors, thus cutting them off from critical resources. However, this will prove extremely difficult to accomplish.

In reality, the U.S. government's ability to regulate international, commercial use of space is likely limited. That said it does have control over its own space-based infrastructure. The U.S. Department of Defense has already identified three focus areas for space mission assurance: defensive operations, resilience and reconstitution.[137] This is a logical focus, which will help safeguard critical military uses of space by defending against attacks where possible, leveraging space systems that are resilient to attack that cannot be defended against, and, if all else fails, being able to quickly replace damaged infrastructure.

Conclusion

This report has demonstrated the need to consider the space domain as part of a multi-domain threat environment, where domains are interconnected and interdependent. In evaluating the particular vulnerabilities that exist in the space-cyber nexus, it finds that increasingly sophisticated technologies that rely on archaic and insecure communications networks are particularly problematic and open to exploitation by MNSAs. Furthermore, this research provides myriad potential, future scenarios where military and commercial interests that rely on space-based systems can be compromised due to vulnerabilities in space-based systems.

In disaggregating MNSAs by motivation and capabilities, it seems likely that of all the types of actors, cyber warriors backed by nation states have the greatest potential and interest to interfere in space. It is also apparent that violent extremists have the most limited capabilities. Nevertheless, they do have much to gain by exploiting space-based technologies. Importantly, this research also demonstrates that collaboration between disparate group types is likely. As such, even less capable groups could perpetrate complex attacks.

Finally, the proliferation of space-based technology, absent strong regulation and coupled with increasing reliance on space-based infrastructure, will continue to make space an attractive target for MNSAs. This is especially likely to be the case as the capabilities gap between the United States and MNSAs in other, more conventional areas of competition widens.

[137] Cihan Erban and Izzet Kale, "The Role of space in the security and defense policy of Turkey. A change in outlook: security in space versus security from space," Science Direct, Space Policy, 2017, http://refhub.elsevier.com/S0265-9646%2816%2930079-0/sref35.

References

"2011 Report to Congress of the U.S.-China Economic and Security Review Commission." One Hundred and Twelfth Congress, November 2011. https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf.

Al-Bayati, T. Hamid. "Introduction: From Al-Qaeda To The Islamic State (ISIS), Jihadi Groups Engage in Cyber Jihad: Beginning With 1980s Promotion Of Use Of 'Electronic Technologies' Up To Today's Embrace Of Social Media To Attract A New Jihadi Generation." *The Middle East Media Research Institute,* (IOS Press Ebooks, 2014).

Alkhouri, Laith; Kassirer, Alex and Nixon, Allison. "Hacking for ISIS: The Emergent Cyber Threat Landscape." A report for Flashpoint, April 2016. https://fortunascorner.com/wp-content/uploads/2016/05/Flashpoint_HackingForISIS_April2016-1.pdf.

Arthur, Charles. "Chinese Hackers Suspected of Interfering with US Satellites." The Guardian, October 27, 2011. https://www.theguardian.com/technology/2011/oct/27/chinese-hacking-us-satellites-suspected.

BBC News, "Poor Coding Limits IS hackers; cyber-capabilities, says researcher," September 25, 2017, http://www.bbc.com/news/technology-41385619.

Beers, Rand and Taylor, Francis X. U.S. State Department, "Narco-Terror: The Worldwide Connection Between Drugs and Terror." testimony before the U.S. Senate Judiciary Committee, Subcommittee on Technology, Terrorism, and Government Information, March13, 2002.

Bergal, Jenni. "Hacktivists Increasingly Target Local and State Government Computers." Huffington Post, January 11, 2017. https://www.huffingtonpost.com/entry/hacktivists-increasingly-target-local-and-state government_us_587651e8e4b0f8a725448401.

Bergal, Jenni. "Hacktivists launch more cyberattacks against local, state governments." PBS News Hour, January 10, 2017. https://www.pbs.org/newshour/nation/hacktivists-launch-cyberattacks-local-state-governments.

Burgess, Matt. "Hackers targeting satellites could cause 'catastrophic; damage." *Wired,* September 22, 2016. http://www.wired.co.uk/article/satellites-vulnerable-hacking-chatham-house.

Carter, Terry. "Organized crime leaders and terrorists cross paths in cyberspace." *ABA Journal,* January 2014. http://www.abajournal.com/magazine/article/organized_crime_leaders_and_terrorists_cross_paths_in_cyberspace.

Chariton, John. "Al Qaeda buys cyber criminal expertise." *Computer Fraud & Security* 2005, no. 3 (2005): 2.

Clapper, James. "Worldwide Threat Assessment of the US Intelligence Community." Senate Armed Services Committee, (Washington, D.C., 2016.).

Cloherty, Jack. "Virtual Terrorism: Al Qaeda Video calls for 'electronic jihad'." *ABC News,* May 22, 2012, http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875.

CNN Wire Staff, "U.S. Senators: Al Qaeda calls for 'electronic jihad'," CNN, May 23, 2012, http://www.cnn.com/2012/05/23/politics/al-qaeda-electronic-jihad/index.html

Corera, Gordon. "Iran building permanent military base in Syria – claim." BBC News, November 10, 2017. http://www.bbc.com/news/world-middle-east-41945189.

Curtis, Glenn and Karacan, Tara. "The Nexus Among Terrorists, Narcotics Traffickers, Weapons Proliferators, and Organized Crime Networks in Western Europe." A study prepared by the Federal Research Division, Library of Congress, December 2002. 22, [http://www.loc.gov/rr/frd/pdf-files/WestEurope_NEXUS.pdf.

D'Alfonso, Steven ."Why Organized Crime and Terror Groups Are Converging." Security Intelligence, September 3, 2014. https://securityintelligence.com/why-organized-crime-and-terror-groups-are-converging/.

De Wet, Dawie. "Satellite networks could prove key to the financial services industry." *Memeburn,* September 1, 2015. https://memeburn.com/2015/09/satellite-networks-could-prove-key-to-the-financial-services-industry/.

Denning, Dorothy. "The Rise of Hacktivism." *Georgetown Journal of International Affairs,* 2015.

Earnhardt, Rebecca; Ackerman, Gary; Halverson, James; Craig, Helena and Hoodjer, Steve. "Terrorist Technology Transfer." Final Report. College Park, MD: START, 2017.

Erban, Cihan and Kale, Izzet. "The Role of space in the security and defense policy of Turkey. A change in outlook: security in space versus security from space." Science Direct, Space Policy, 2017. http://refhub.elsevier.com/S0265-9646%2816%2930079-0/sref35.

"Hack a Satellite While It is in Orbit." Toolbox Tech, https://it.toolbox.com/blogs/rmorril/hack-a-satellite-while-it-is-in-orbit-041307.

Franceschi-Bicchierai, Lorenzo. "This $1,000 Device Lets Hackers Hijack Satellite Communications." *Motherboard,* July 31, 2015.

Goodman, Marc. *Future Crimes : Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It*. First Edition. ed. New York: Doubleday, 2015.

Graham-Harrison, Emma. "Could Isis's 'cyber caliphate' unleash a deadly attack on key targets?" The Guardian. April 12, 2015. https://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race.

Halterman, TE. "Terrain2STL Lets Users 3D Print Topographic Maps from Google Maps Data." 3DPrint.com, July 21, 2015, https://3dprint.com/83026/terrain2stl-3d-print-maps/.

Hampson, Joshua. "The Future of Space Commercialization." Research Paper (Niskanen Center, 2017). https://science.house.gov/sites/republicans.science.house.gov/files/documents/TheFutureofSpaceCommercializationFinal.pdf.

Hesterman, Jennifer. *The Terrorist Criminal Nexus: An Alliance of International Drug Cartels, Organized Crime, and Terror Groups.* (Boca Raton: CRC Press, 2013).

Hill, Kashmir. "Jamming GPS Signals is Illegal, Dangerous Cheap and Easy. " Gizmodo, July 24, 2017. https://gizmodo.com/jamming-gps-signals-is-illegal-dangerous-cheap-and-e-1796778955.

Ignatius, David. "War in Space is Becoming a Real Threat," The Washington Post, March 16, 2017. https://www.washingtonpost.com/opinions/war-in-space-is-becoming-a-real-threat/2017/03/16/af3c35ac-0a8f-11e7-a15f-a58d4a988474_story.html?utm_term=.c43d4ab32f5c.

Iridium Hacking, Please don't sue us," https://media.ccc.de/v/camp2015-6883-iridium_hacking#t=1427

Ismail, Nick. "Defending against cyber attacks is now just as important as the fight against terror – GCHQ," Information Age, October 9, 2017. http://www.information-age.com/cyber-security-threat-just-serious-terrorism-gchq-123468981/.

Ismail, Nick. "Money, terrorism or nation state snooping – how understanding the real motives behind cyber attacks can help to prevent them." *Information Age,* June 30, 2017. http://www.information-age.com/understanding-motives-behind-cyber-attacks-can-help-prevent-123467078/.

Kaaman, Hugo. "The History and Adaptability of the Islamic State Car Bomb." Blog Post, February 14, 207. https://zaytunarjuwani.wordpress.com/2017/02/14/the-history-and-adaptability-of-the-islamic-state-car-bomb/islamic.

Kahn, Jeremy. "Mumbai Terrorists Relied on New Technology for Attacks." The New York Times, December 8, 2008.

http://www.nytimes.com/2008/12/09/world/asia/09mumbai.html?mtrref=www.google.com&gwh=1A0ABEBE14584DB43045B32BD9C8D40B&gwt=pay.

"Kessler Syndrom". http://gravitymovie.wikia.com/wiki/Kessler_Syndrome.

Khandelwal, Swati. "Russian Hackers Hijack Satellite to Steal Data From Thousands of Hacked Computers." The Hacker News, September 10, 2015. https://thehackernews.com/2015/09/hacking-satellite.html.

Kimery, Anthony. "Mumbai Terrorists' Use Of Google Earth Re-Ignites Concerns," Homeland Security Today, Decemer 5, 2008, http://www.hstoday.us/columns/global-watch/blog/mumbai-terrorists-use-of-google-earth-re-ignites-concerns/642770639e0a4ae59d34a79be3a628fa.html.

Kingsbury, Alex. "Documents Reveal Al Qaeda Cyberattacks," *U.S. News,* April 14, 2010. https://www.usnews.com/news/articles/2010/04/14/documents-reveal-al-qaeda-cyberattacks.

Kramer, Andrew. "How Russia Recruited Elite Hackers for Its Cyberwar," The New York Times, December 29, 2016. https://www.nytimes.com/2016/12/29/world/europe/how-russia-recruited-elite-hackers-for-its-cyberwar.html.

Lipton, Eric; Sanger, David E. and Shane, Scott. "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." December 13, 2016. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

Livingsstone, David and Lewis, Patricia. "Space, the Final Frontier for Cybersecurity?" *Chatham House, International Security Department*, September 2016.

Livingstone, Daniel. 'The Intersection of Space and Cybersecurity is a Growing Concern." Chatham House Expert Comment, November 25, 2014.

Lohrman, Dan. "Understanding New Hacktivism: Where Next for Hackers With a Cause." Government Technology, July 31, 2016. http://www.govtech.com/blogs/lohrmann-on-cybersecurity/understanding-new-hacktivism-where-next-for-hackers-with-a-cause.html.

Lyall, Jason. "Does indiscriminate violence incite insurgent attacks? Evidence from Chechnya." *Journal of Conflict Resolution* 53, no. 3 (2009): 331-362.

Mahmood, Riyad Mitieb. "The Mechanism of Deliberate Jammin on the Broadcast Satellite Service." Journal of University of Anbar for Pure Science: 6:2, 2012. https://www.iasj.net/iasj?func=fulltext&aId=63233.

Manzo, Vincent. "Deterrence and Escalation in Cross-domain Operations." *JFQ: Joint Force Quarterly* 66 (2012): 8-14.

Marks, Joseph. "ISIL aims to launch cyberattacks on U.S." Politico, December 29, 2015. http://www.politico.com/story/2015/12/isil-terrorism-cyber-attacks-217179.

Martin, Mel. "SpyMeSat iOS app now lets you buy hi-resolution satellite images." Engadget, July 13, 2014. https://www.engadget.com/2014/06/13/spymesat-ios-app-now-lets-you-buy-hi-resolution-satellite-images/;https://www.spymesat.com/.

Metropolitan.fi, "DDoS attack halts heating in Finland amidst winter," http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter.

Meyers, C.A. Powers, SS and Faissol,D. M. *Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches*. No. LLNL-TR-419041. Lawrence Livermore National Laboratory (LLNL), Livermore, CA, 2009.

Mills, Elinor. "Old-time hacktivists: Anonymous, you've crossed the line." CNet, March 30, 2012. https://www.cnet.com/news/old-time-hacktivists-anonymous-youve-crossed-the-line/.

Morse, Jack. "Remotely hacking ships shouldn't be this easy, and yet ..." *Mashable,* July 18, 2017. https://mashable.com/2017/07/18/hacking-boats-is-fun-and-easy/#KYk3Hm5Q_aqf.

Murdock, Jason. "How Satellite Surveillance is Helping to Predict Stock Prices." Newsweek, March 2, 2017. http://www.newsweek.com/how-satellite-surveillance-helping-predict-stock-prices-skynet-562973.

Murphy, Samantha. "New hacktivist sect emerges from anonymous." New Scientist, April 18, 2012. https://www.sciencedirect.com/science/article/pii/S0262407912610070?via%3Dihub.

Nakashima, Ellen and Gillum, Jack. "Russian government hackers used antivirus software to steal U.S. cyber capabilities." The Washington Post, October 5, 2007. https://www.washingtonpost.com/world/national-security/russian-government-hackers-exploited-antivirus-software-to-steal-us-cyber-capabilities/2017/10/05/a01bf546-a9fc-11e7-92d1-58c702d2d975_story.html?utm_term=.4f099ea41aa8.

Newman, Lily Hay. "Hacker Lexicon: What is the Attribution Problem," Wired, December 24, 2016. https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/.

Olson, Steve. "The Danger of Space Junk." The Atlantic, July 1998. https://www.theatlantic.com/magazine/archive/1998/07/the-danger-of-space-junk/306691/.

Pendergrass, William. *What is anonymous?: a case study of an information systems hacker activist collective movement.* (New York: Penguin Press, 2016), 315–16.

Porup, J.M. "It's surprisingly simple to hack a satellite." Motherboard, April 21, 2014. https://motherboard.vice.com/en_us/article/bmjq5a/its-surprisingly-simple-to-hack-a-satellite.

"Rad1o to hardware overview," https://rad1o.badge.events.ccc.de/hardware:overview

Ranger, Steve. "Organised cybercrime groups are now as powerful as nations. " *ZDNet,* June 9, 2014.

Raymond Choo, Kim-Kwang and Smith, Russell G. "Criminal exploitation of online systems by organized crime groups." *Asian journal of criminology* 3, no. 1 (2008): 37-59.

Ritchell, Matt. "Devices Enforce Silence of Cellphones, Illegally." The New York Times, November 4, 2007. http://www.nytimes.com/2007/11/04/technology/04jammer.html.

Rollins, John. Report to Congress, (2006), https://fas.org/sgp/crs/terror/RL33123.pdf.

Saadawi, Tarek and Colwell, John Jr. *Cyber infrastructure Protection Volume III.* (Carlisle:Army War College-Strategic Studies Institute Carlisle United States, 2017), 15.

Seebruck, Ryan. "A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model." *Digital Investigation* 14 (2015): 36-45.

Shachtman, Noah. "How Gadgets Helped Mumbai Attackers." Wired, December 1, 2008. https://www.wired.com/2008/12/the-gagdets-of/.

Shelley, Louise, Picarelli, John, Irby, Allison, Hart, Douglas M., Craig-Hart, Patricia, Williams, Phil, Steve Simon, Abdullaev, Nabi, Stanislawski, Bartosz, and Covill, Laura. "Methods and Motives: Exploring Links between Transnational Organized Crime & International Terrorism." A report for the U.S. Department of Justice, June 23, 2005.

"Sri Lankan Terrorists Hack Satellite." Impact Lab, http://www.impactlab.net/2007/04/13/sri-lankan-terrorists-hack-satellite/.

Stalinsky, Steven and Sosnow, R. "From Al-Qaeda To The Islamic State (ISIS), Jihadi Groups Engage in Cyber Jihad: Beginning With 1980s Promotion Of Use Of 'Electronic Technologies' Up To Today's Embrace Of Social Media To Attract A New Jihadi Generation." *The Middle East Media Research Institute,* (IOS Press Ebooks, 2014).

Subrahmanian, V.S.; Mannes, Aaron; Silva, Amy; Shakarian, Jana, and Dickerson. John P.. "A Brief History of LeT." In *Computational Analysis of Terrorist Groups: Lashkar-e-Taiba*, (New York: Springer, 2013), pp. 23-68.

UK HM Government (2014), "National Space Security Policy." UKSA/13/1292, 2. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307346/National_Space_Security_Policy.pdf.

Warren, Peter. *Cyber Alert: How the World is Under Attack from a New Form of Crime (*Vision, 2005).

Waters, Nick. "Types of Islamic State Drone Bombs and Where to Find Them." *Belingcat,* May 24,2017. https://www.bellingcat.com/news/mena/2017/05/24/types-islamic-state-drone-bombs-find/.

Wax, Emily. "Mumbai Attackers Made Sophisticated Use of Technology." Washington Post Foreign Service, December 3, 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/12/02/AR2008120203519.html.

Weng, Qihao. "Remote sensing of impervious surfaces in the urban areas: Requirements, methods, and trends." *Remote Sensing of Environment* 117 (2012): 34-49.

"Who is Anna-Senpai, the Mirai Worm Author?" Krebs on Security, January 2017. https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/.

Williams, Phil and Fiddner, Dighton. *Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition.* (Carlisle:Army War College-Strategic Studies Institute Carlisle United States, 2016).

Williams, Phil; Reuter, Peter; Arthur, Richard; Cliff, William and Ackerman, William. *The Potential Nexus Between Organized Criminals, Terrorists and Radiological Nuclear Smuggling: A Theoretical Discussion.* (START: College Park, MD, 2011).

Wired, "The Biggest Security Threats Coming in 2017." January 2, 2017. https://www.wired.com/2017/01/biggest-security-threats-coming-2017/.

Wolf, Jim. "China Key suspect in U.S. satellite hacks: commission." *Reuters,* October 28, 2011. china-usa-satellite-idUSN1E79R1LK20111028.

Woody, Christopher. "The Navy's 4th accident this year is stirring concerns about hackers targeting US warships." Business Insider, August 24, 2017. http://www.businessinsider.com/hacking-and-gps-spoofing-involved-in-navy-accidents-2017-8.

Woolf, Nicky. "DDoS attack that disrupted internet was largest of its kind in history, experts say," *The Guardian,* October 26, 2016.

Zenko, Micah. "Dangerous Space Incidents." Contingency Planning Memorandum (Council on Foreign Relations: New York) 2014, 3).

Zetter, Kim. "Hackers Could Heist Semis by Exploiting This Satellite Flaw." Wired, July 30, 2016. https://www.wired.com/2015/07/hackers-heist-semis-exploiting-satellite-flaw/.