2021 13th International Conference on Cyber Conflict
Going Viral
T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.)
2021 © NATO CCDCOE Publications, Tallinn

Adversary Targeting of Civilian Telecommunications Infrastructure

Keir Giles
Conflict Studies Research Centre
Northamptonshire, United Kingdom
keir.giles@conflictstudies.org.uk

Kim Hartmann
Conflict Studies Research Centre
Northamptonshire, United Kingdom
kim.hartmann@conflictstudies.org.uk

Abstract: The response to the pandemic by states, organisations, and individuals in 2020 highlighted critical dependency on communications systems underpinned by cyber infrastructure. Without the benefits of connectivity, governments would have faced greater challenges governing, societies would have found it even harder to maintain cohesion, more companies would have ceased to operate altogether, and personal isolation would have been a vastly more difficult experience.

And yet, it is precisely this connectivity within and between NATO states that some adversaries are preparing to attack in time of conflict, including through physical or kinetic means. Russia in particular has long invested in probing vulnerabilities of civilian internet and telecommunications infrastructure, and this programme was urgently ramped up to unprecedented levels of intensity after the seizure of Crimea in 2014 demonstrated the power of total information dominance achieved through targeting critical information assets.

Besides Russia, China and a number of other states are also rapidly developing counter-space capabilities that would pose a direct threat to critical civilian communications services. This has obvious implications for crisis management even before overt state-on-state conflict. Vulnerabilities have been sought in all domains: maritime (subsea cables), space (communications satellites), land (fibre optic nodes), and online (targeting specific media sources for neutralisation). The VPNFilter malware exposed in mid-2018, in addition to its cybercrime or cyber-espionage capabilities, demonstrated the ambition to render large numbers of ordinary users in NATO countries simply unable to communicate.

Recognising and responding to this emerging disruptive threat and its potential human, societal, and state impact is critical to the defence of NATO states – still more so in the case of disruption to normal life by events such as the pandemic. The threat to cyber-

physical systems not ordinarily considered a military target must be recognised, and their defence and security prioritised. This paper outlines the threat and recommends a range of mitigation strategies and measures.

Keywords: *information warfare, infrastructure, space, satellites, telecommunications, Russia, China*

1. INTRODUCTION

"In the modern era you can achieve the same effect as used to be achieved in, say, World War Two by bombing the London docks or taking out a power station, by going after the physical infrastructure of cyberspace."

Mark Sedwill, former National Security Adviser, UK Cabinet Office [1]

On Christmas Day 2020, a suicide vehicle-borne improvised explosive device (SVBIED) detonated in central Nashville, Tennessee, next to a facility operated by telecoms provider AT&T.[2] The incident "brought communications in the region, from Georgia to Kentucky, to a halt, affecting 911 call centers, hospitals, the Nashville airport, government offices and individual mobile users… businesses big and small". The extent of the communications failures and subsequent disruption demonstrated not only that the AT&T facility represented a single point of failure for telecommunications networks across an extensive area of the United States, but also that local and regional government offices and essential services had no fallback options for maintaining communications.[3]

The Nashville attack is considered an isolated incident, carried out by a single troubled individual. But the vulnerability and lack of resilience demonstrated by this one event will have been of intense interest to nation states that wish harm to the United States and its allies, and in particular, to those that in time of conflict aim to target critical information infrastructure and the connectivity it provides. The disruption caused by one attack would be substantially increased by a simultaneous, coordinated campaign

1 "Joint Committee on the National Security Strategy", 18 December 2017, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/work-of-the-national-security-adviser/oral/75927.pdf

2 Kimberlee Kruesi, Michael Balsamo, and Eric Tucker, "Downtown Nashville Explosion Knocks Communications Offline", AP, 25 December 2020, https://apnews.com/article/Nashville-explosion-Christmas-52708bfd05e4f6ff433cc404443c65d4

3 Yihyun Jeong and Natalie Allison, "Nashville Bombing Exposed 'Achilles Heel' in Area Communications Network", *Nashville Tennessean*, 29 December 2020, https://www.tennessean.com/story/news/local/2020/12/29/nashville-bombing-area-communications-network-exposed-achilles-heel/4062089001/

against key information nodes, presenting a serious challenge to governance and the normal functioning of society in the victim state.

This paper considers the challenge of direct intervention against physical infrastructure in the context of a cyber, information, or conventional conflict. It reviews the stated or implicit ambition of adversaries to achieve information dominance, disruption, or destruction through action against civilian telecommunications infrastructure during or before overt conflict, and the implications for NATO nations. Sections review adversary activities toward this end in different domains: space, subsea, on land, and online. The paper then concludes with a set of proposed means of mitigating a range of vulnerabilities.

A. Dependence on Connectivity

The response to the pandemic by states, organisations, and individuals in early 2020 highlighted the critical dependency of societies on communications systems underpinned by cyber infrastructure. Without the benefits of hyperconnectivity, governments would have faced greater challenges governing, communities would have found it even harder to maintain cohesion, more private sector companies would have ceased to operate altogether, and personal isolation would have been a vastly more difficult and unpleasant experience. But even in normal times, dependence on always-on internet and telecommunications in many states has grown to the point that their denial or interdiction would cause severe challenges.

A number of distinct phenomena exacerbate this problem. First, the assumption that internet access is a normal default state leads to a neglect of redundancy and resilience, such that when, for example, Google services are briefly unavailable, large numbers of organisations find their normal business entirely paralysed.[4] Second, the ongoing rollout of the internet of things (IoT) has at times been accompanied by insufficient consideration of fallback modes for communications outages. This means that when backbone providers such as Amazon Web Services are disrupted, the impact is not only on commerce, logistics, media outlets and governance, but also on families finding their smart homes and smart devices have stopped working.[5] Furthermore, malign actors taking remote control of connected devices with no failsafes will increasingly present severe challenges to everyday activities.[6] Third, on an individual level,

4 "Google Cloud Infrastructure Components Incident #20013", Google, 14 December 2020, https://status.cloud.google.com/incident/zall/20013; Erika Varagouli, "'Google Down': How Users Experienced Google's Major Outage", Semrush, 15 December 2020, https://www.semrush.com/blog/google-down-how-users-experienced-google-major-outage/

5 Jay Greene, "Amazon Web Services outage hobbles businesses", *Washington Post*, 25 November 2020, https://www.washingtonpost.com/business/economy/amazon-web-services-outage-stymies-businesses/2020/11/25/b54a6106-2f4f-11eb-860d-f7999599cbc2_story.html; "AWS: Amazon web outage breaks vacuums and doorbells", BBC, 26 November 2020, https://www.bbc.co.uk/news/technology-55087054

6 Lorenzo Franceschi-Bicchierai, "We Spoke to a Guy Who Got His Dick Locked in a Cage by a Hacker", *Vice*, 28 January 2021, https://www.vice.com/en/article/4ad5xp/we-spoke-to-a-guy-who-got-his-dick-locked-in-a-cage-by-a-hacker

reliance on connected devices has led to an atrophy of skills required for when they are not available. This has been primarily highlighted to date in one of the clearest and simplest examples: the growing inability not only among the general public but even among military recruits to read maps and thus be able to navigate when disconnected.[7]

Until now, the incidents that demonstrate these vulnerabilities have been isolated, brief, and the result of technical errors or natural incidents rather than deliberate attack – but as with the Nashville blast, they give an indication of the potential damage if the reverse were true. The impact of this kind of attack would vary between NATO nations and even within them: the vulnerability will be even greater in countries with high degrees of connectivity and extensive adoption of near-universal online government and financial services, such as Estonia, than in countries that are relatively backward in this regard, such as the United States.[8] But in all cases, both the opportunities for carrying out this kind of attack and its probable impact are greatly increased if the attractiveness of civilian telecommunications infrastructure as a target for adversaries is underestimated.

B. Russia

The state that has most clearly acted on this attractiveness is Russia. The underlying principles of attacks on communications nodes are neither unique nor new, but it is primarily Russia that has both demonstrated and learned from the value in modern conflict of kinetic attacks that facilitate information outcomes, as opposed to the reverse.

Recent shifts in Russian thinking about the potential power of information warfare go to the heart of how wars are won: whether by destroying the enemy, or by rendering the enemy unable to fight.[9] For the latter purpose, the use of information operations against adversary populations and societies is part of an unbroken tradition in the institutional culture of Russia's military, intelligence, and political leadership that reaches back not only into Communist times but even before.[10] This includes information interdiction. In the current century this has been exercised via the internet: the socio-cyber attacks on Estonia in 2007 included crude attempts at cutting communications between government and citizens and with the outside world, modified and implemented with greater success against Georgian government communications the following

7 Danielle Sheridan, "Soldiers Must Know How to Read Maps Because Satellites Could Be Lost, Commander Field Army Says", *Daily Telegraph*, 4 December 2020, https://www.telegraph.co.uk/news/2020/12/04/soldiers-must-know-read-maps-satellites-could-lost-commander/

8 Olga Khazan, "America's Terrible Internet Is Making Quarantine Worse", *Atlantic*, 17 August 2020, https://www.theatlantic.com/technology/archive/2020/08/virtual-learning-when-you-dont-have-internet/615322/

9 Keir Giles, "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power", Chatham House, March 2016, https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf

10 Bilyana Lilly and Joe Cheravitch, "The Past, Present, and Future of Russia's Cyber Strategy and Forces", 2020 12th International Conference on Cyber Conflict, May 2020, https://www.ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf

year.[11] But the prehistory of this kind of operation includes the traditional seizure or destruction of civilian broadcast facilities and telephone and telegraph exchanges at the first stage of any attempt at regime change, whether imposed from abroad or by notionally domestic actors – as exemplified by a previous Moscow-backed attack on Estonia, the attempted coup in 1924.[12] Similarly, during the Cold War, part of the mission of KGB and GRU (Main Intelligence Directorate) sabotage teams inserted into Western countries was to seize or destroy communications and radio and TV broadcasting facilities.[13]

The extension of this principle into targeting internet infrastructure had been flagged in Russian conceptual writing on information warfare. An authoritative analysis of the new capabilities required by Russia following the armed conflict in Georgia in 2008 noted that "it is necessary to develop a centre for the determination of critically important information entities of the enemy, including how to eliminate them physically".[14] As in other cases, realisation of the offensive potential of operations of this kind was accompanied, or perhaps driven, by recognition of Russia's own previous vulnerability in this regard. The security and intelligence agencies' calls for greater attention to information security were in part founded on the concerns that "destruction and disorganisation of information infrastructure… on the scale of weapons of mass destruction is possible".[15]

But it was the seizure of Crimea in 2014 that provided a case study of information dominance facilitating an almost bloodless geopolitical gain, and consequently gave substantial impetus to Russia's interest in the potential vulnerabilities of NATO allies' civilian communications infrastructure. After gradually establishing control over traditional media in the days leading up to the operation to take the peninsula, Russian troops took over the Simferopol Internet Exchange Point and telecommunications cable connections to the mainland.[16] Together these operations gave Russia complete control of the Crimean information space, isolating it from the outside world.[17] The result was public perception of events in Crimea being determined exclusively by

11 Sean Ainsworth, "The Evolution of the Russian Way of Informatsionnaya Voyna", in Reuben Steff et al. (editors), *Emerging Technologies and International Security: Machines, the State, and War* (Routledge, 2020), pp. 137–152.

12 Merle Maigre, "Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO", German Marshall Fund of the United States (GMF) Policy Brief, February 2015, p. 2.

13 "The Soviet Army: Specialized Warfare and Rear Area Support", FM 100-2-2, US Army, 16 July 1984, p. 5-4.

14 "Russia is Underestimating Information Resources and Losing out to the West", *Novyy Region*, 29 October 2008.

15 Vladimir Markomenko, "Невидимая затяжная война" (Invisible protracted war), *Nezavisimoye voyennoye obozreniye*, No. 30, 16 August 1997.

16 "Кримські регіональні підрозділи ПАТ 'Укртелеком' офіційно повідомляють про блокування невідомими декількох вузлів зв'язку на півострові" (Crimean regional divisions of PJSC "Ukrtelecom" officially report the blocking of several communication nodes on the peninsula by unknown persons), Ukrtelekom, 28 February 2014, https://www.scm.com.ua/news/ukrtelecom-s-statement

17 Shane Harris, "Hack Attack. Russia's First Targets in Ukraine: Its Cell Phones and Internet Lines", *Foreign Policy*, 3 March 2014, http://foreignpolicy.com/2014/03/03/hack-attack/

Russia, which contributed greatly to preventing resistance to the takeover by the civilian population.

The operation showed that advanced cyber capabilities are not necessary to achieve total control of an internet and telecommunications network if it is possible to mount a physical intervention against network infrastructure, the reverse of the more commonly considered scenario where cyber vulnerabilities are exploited for damaging physical effect.[18] This recognition appears to lie behind an intense and urgent subsequent pattern of activity by Russian military and intelligence organisations directed at civilian internet and telecommunications facilities across multiple continents. The end goal may be to interdict information through use of cyber, electronic warfare (EW), or kinetic activity, denying NATO governments the ability to communicate with their citizens in time of conflict and denying populations access to outside information, in an attempt to replicate the success delivered by total information dominance in Crimea. But even if Russia's objectives are limited to the military aims of denying, disrupting, or degrading NATO's ability to communicate, navigate, and target opposing forces, attempts to do so through destructive intervention against internet infrastructure would have profound second- and third-order effects on civil society during even a brief confrontation.

The remainder of this paper therefore considers the various domains in which threats to the infrastructure underpinning civilian internet and telecommunications services arise: subsea, in space, on land (including by electronic warfare), and in cyber and information space. Throughout, it should be remembered that the nature of the threat will vary between adversaries, because not all adversaries are identical and they will play to their strengths; for instance, the potential abuse of hardware and firmware dominance by China in Western telecommunications networks is an enduring source of concern, but Russia does not have the kind of ICT (information and communications technology) sector that would allow it to use a comparable vector of attack. Specifically considering preparation for physical interventions against civilian infrastructure, although Russia is not the only state with apparent ambitions of this kind, it is Russian actions that are by far the most widely reported. It is probably not possible to determine from open sources why this is so – whether other countries attach lesser importance to mapping the infrastructure of their potential adversary in this way, or whether, conversely, they ascribe greater importance to doing so in a manner that remains undetected.

18 Owen Matthews, "Russia's Greatest Weapon May Be Its Hackers", *Newsweek*, 5 July 2015, http://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html

2. INFORMATION INTERDICTION

A. Subsea

In the period after the seizure of Crimea, Russia appeared to prioritise other concerns, such as speed, over remaining unobserved. This was especially apparent in the case of the first Russian activities that came to widespread public notice, namely investigation of subsea communications cables for either intelligence exploitation or disruption. The Russian agency primarily responsible for this, the *Glavnoye upravleniye glubokovodnykh issledovaniy* (Main Directorate for Deep-Water Research, GUGI), is a highly secretive organisation that until 2014 operated with such stealth that its purpose, and even its existence, very rarely appeared in open sources.[19] After Crimea, however, the apparent urgency of the task meant GUGI and its vessels attracted sufficient attention that they routinely featured in public reporting in the West.[20]

Concern rose that Russia was seeking the ability to choke off vital international communication channels at will, a task made easier by the fact that the majority of subsea cables are privately owned and their locations publicly known. Submarine cables carrying data, and in some cases those carrying power, present critical vulnerabilities to destructive intervention, with the potential for enormously damaging economic as well as societal disruption.[21] Targeting them would meet a wide range of Russian objectives; according to former SACEUR (Supreme Allied Commander Europe) Jim Stavridis, these would include "a rich trove of intelligence, a potential major disruption to an enemy's economy and a symbolic chest thump for the Russian Navy".[22] While the problem is potentially global in scope, Russian activities around the continental United States, with the potential to tap or disrupt US communications with Europe and Asia, received the majority of public attention and have been claimed to be one of the spurs for the creation of NATO Atlantic Command.[23]

B. Space

By contrast with subsea activities, which remain generally invisible, potentially hostile activity in space is more easily documented thanks to its greater visibility to private,

19 Andrey Soyustov, "ГУГИ против США: 'скрытая угроза' и невидимый фронт" (GUGI against the USA: the 'hidden threat' and the invisible front), Federalnoye agentstvo novostey, 27 October 2015, https://riafan.ru/455430-gugi-protiv-ssha-skryitaya-ugroza-i-nevidimyiy-front

20 See, for instance, David E. Sanger and Eric Schmitt, "Russian Ships Near Data Cables Are Too Close for US Comfort", *New York Times*, 25 October 2015, https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html

21 Rishi Sunak, "Undersea Cables: Indispensable, Insecure", Policy Exchange, November 2017, https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf

22 Jim Stavridis, "A New Cold War Deep Under the Sea?", *Huffington Post*, 28 October 2015, http://www.huffingtonpost.com/admiral-jim-stavridis-ret/new-cold-war-under-the-sea_b_8402020.html

23 Michael Birnbaum, "Russian Submarines Are Prowling around Vital Undersea Cables. It's Making NATO Nervous", *Washington Post*, 22 December 2017, https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html; Alexandra Brzozowski, "NATO Seeks Ways of Protecting Undersea Cables from Russian Attacks", Euractiv.com, 23 October 2020, https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/

commercial, and amateur interests involved in or observing space operations. This leads to a preponderance of open source information on threats in space compared to other domains.[24]

In a worst-case scenario, a peer or near-peer adversary could in theory use both land- and space-based anti-satellite (ASAT) weapons systems to launch a mass attack on satellites, targeting the situational awareness of governments and military forces potentially globally, and their ability to communicate, navigate, and target opposing forces – and triggering catastrophic disruption and lasting damage to the space environment. But more discriminate and selective counter-space effects are also possible. Civilian and military communications satellites can be targeted through a wide range of interventions both from ground level and from space itself, including both kinetic and directed-energy attacks.[25] According to General John W "Jay" Raymond, Chief of Space Operations, US Space Force, both Russia and China have "a menu of counter space effects (kinetic, lasers, jammers, cyber)".[26] Iran, North Korea, and India have also developed different techniques to attack or disrupt satellites.[27]

A standard taxonomy of counter-space capabilities includes:

- Co-orbital ASAT;
- Direct Ascent ASAT;
- Electronic Warfare;
- Directed Energy;
- Cyber Attacks.[28]

Co-orbital ASAT capabilities are intended to collide with, damage, or otherwise neutralise their targets. Unusual manoeuvres by Russian space vehicles observed in the vicinity of communications satellites could be practice for attack runs for deploying anti-satellite weapons in order to degrade Western communications at a critical moment,[29] or, in the most charitable explanation, simply an opportunity for close observation and investigation of Western satellites.[30] Russia's Olymp-K or Luch

24 See, for example, Brian Weeden and Victoria Samson (editors), "Global Counterspace Capabilities: An Open Source Assessment", Secure World Foundation, April 2020; "Seeking Strategic Advantage: How Geopolitical Competition and Cooperation Are Playing Out in Space", Wilson Center, 6 October 2020, https://www.wilsoncenter.org/event/seeking-strategic-advantage-how-geopolitical-competition-and-cooperation-are-playing-out

25 Leonard David, "China, Russia Advancing Anti-Satellite Technology, US Intelligence Chief Says", Space.com, 18 May 2017, https://www.space.com/36891-space-war-anti-satellite-weapon-development.html

26 Speaking at "Defence Space 2020", 17 November 2020, https://www.airpower.org.uk/defence-space-2020/

27 Todd Harrison et al., "Space Threat Assessment 2020", CSIS, March 2020, https://aerospace.csis.org/wp-content/uploads/2020/03/Harrison_SpaceThreatAssessment20_WEB_FINAL-min.pdf

28 Brian Weeden, "Current and Future Trends in Chinese Counterspace Capabilities", *IFRI Proliferation Papers* 62, November 2020.

29 Patrick Tucker, "Russia Tests a Satellite That Rams Other Satellites, US Says", *Defense One*, 23 July 2020, https://www.defenseone.com/technology/2020/07/russia-tests-satellite-rams-other-satellites-us-says/167154/

30 Brian Weeden, "Dancing in the Dark Redux: Recent Russian Rendezvous and Proximity Operations in Space", *Space Review*, 5 October 2015, http://www.thespacereview.com/article/2839/1

satellite has attracted particular attention by approaching 11 unique Intelsat satellites, four Eutelsat satellites, two SES satellites, and at least nine other satellites operated by Russia, Turkey, Pakistan, the United Kingdom, and the European Space Agency since its launch in September 2014.[31]

By contrast, direct ascent ASAT systems consist of a missile with a kill vehicle launched from land, aircraft, or ship, which collides with the target satellite at high speed and obliterates both objects. Russia has extensively tested weapons of this kind, developed from missile defence systems.[32] And in early 2019, India became the fourth country after the US, China, and Russia to successfully test a ground-launched ASAT missile.[33]

Non-kinetic counter-space capabilities include the use of laser, microwave, and electromagnetic pulse energy against space systems. Anti-satellite EW capabilities can offer interference, denial, and manipulation of radio frequencies operations against satellite and ground support systems.[34] This can also spoof signals from satellites, or simply make it difficult to detect them. Meanwhile, lasers capable of dazzling sensors on satellites could, at greater power, potentially cause physical damage.[35]

And at the juncture of the domains of space and cyber, cyber counter-space operations include capture, disruption, and denial operations against satellite systems through the exploitation of digital vulnerabilities.[36] Unlike electronic attacks, which would prevent satellites communicating, cyber attacks could use the communication channels to deliver corrupted data or malicious commands. Satellite ground stations and their associated communications services would be potential entry points for cyber attacks, while targeting a satellite's command and control system could damage or destroy the satellite, or remove it from orbit.[37] Vulnerabilities to attack have also been found in satellite communications (SATCOM) data links, critically important to military C5ISR

31 Thomas G. Roberts, "Unusual Behavior in GEO: Luch (Olymp-K)", Aerospace Security Project, CSIS, accessed 1 March 2020, https://aerospace.csis.org/data/unusual-behavior-in-geo-olymp-k/

32 "Russia Tests Direct-Ascent Anti-Satellite Missile", US Space Command, 16 December 2020, https://www.spacecom.mil/News/Article-Display/Article/2448334/russia-tests-direct-ascent-anti-satellite-missile/; see also Keir Giles, "Russian Ballistic Missile Defense: Rhetoric And Reality", US Army War College Strategic Studies Institute, June 2015, https://ssi.armywarcollege.edu/russian-ballistic-missile-defense-rhetoric-and-reality/

33 Shaan Shaikh, "India Conducts Successful ASAT Test", Missile Threat, CSIS, 28 March 2019, https://missilethreat.csis.org/india-conducts-successful-asat-test/

34 Todd Harrison et al., "Space Threat Assessment 2018", CSIS, April 2018, https://www.csis.org/analysis/space-threat-assessment-2018

35 Noah Shachtman, "Is This China's Anti-Satellite Laser Weapon Site?" *Wired*, 11 March 2009, https://www.wired.com/2009/11/is-this-chinas-anti-satellite-laser-weapon-site/

36 Rajeswari Pillai Rajagopalan, "Electronic and Cyber Warfare in Outer Space", UNIDIR, May 2019, p. 1–11, https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf; see also Beyza Unal, "Cybersecurity of NATO's Space-based Strategic Assets", Chatham House, July 2019, https://www.chathamhouse.org/2019/07/cybersecurity-natos-space-based-strategic-assets

37 In addition, Russia is believed to have successfully exploited foreign satellites and their unencrypted communications with ground receiver stations as part of a broader cyber campaign. See Sam Jones, "Russian Group Accused of Hacking Satellites", *Financial Times*, September 2015. Available at: https://www.ft.com/content/50b1ff84-571d-11e5-9846-de406ccb37f2

(Command, Control, Communication, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance), transport, industry, and especially aviation technology, where these systems are indispensable.[38] Cyber vulnerabilities in satellite receiving stations also pose secondary risks, as many operational services dependent on data from satellites (for instance, weather services) are distributed via ground station links.[39]

In addition to their effects on civilian communications and other services, targeting of space assets for military effect in conventional conflict is also a substantial risk. US and NATO forces are highly dependent on space-based systems for situational awareness, communication, navigation, and targeting of opposing forces. Degradation or destruction of space assets would put expeditionary forces deploying over long distances at a particular disadvantage relative to the adversary, who would already be present at the edge of the battlespace. Meanwhile, interference with Global Positioning System (GPS) services would negate the effectiveness of GPS-dependent navigation systems and standoff weapons, and dazzling or destruction of surveillance and imaging satellites would prevent observation of the buildup and manoeuvre of adversary forces.

This means that adversaries possessing sufficiently advanced technical capabilities have a strong incentive to target satellites as a key vulnerability.[40] According to Air Chief Marshal Sir Mike Wigston, Chief of Air Staff, RAF, "Future conflict may not start in space, but it may transition quickly to space and it may be won or lost in space".[41] One authoritative assessment of Russian doctrinal and capability developments notes that "Russia considers space as a theater of military operations… Therefore, the emergence of new forms of military operations in near space can be expected".[42] Russia may also view activities in space as a potential component of non-nuclear deterrence, presenting a means of holding high-value adversary targets at risk as an alternative to strategic non-nuclear strike weapons.[43]

C. Land

Denial of access to cyberspace for a targeted region or nation could include physical operations to inflict damage to vital information technology infrastructure on land, such as fibre-optic cables, server farms, terrestrial communication lines, wireless

38 Ruben Santamarta, "SATCOM Terminals: Hacking by Air, Sea, and Land", IOActive, 2014, https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf

39 Mike Gruss, "Report Cites Vulnerability in NOAA's Satellite Ground Stations", *Space News*, August 2014, https://spacenews.com/41685report-cites-vulnerability-in-noaas-satellite-ground-stations/

40 Caroline Houck, "The US Army Knows It's Vulnerable to Space Attack. Here's What They Want to Do About It", *Defense One*, 4 December 2017, http://www.defenseone.com/technology/2017/12/us-army-knows-its-vulnerable-space-attack-heres-what-they-want-do-about-it/144279/

41 Speaking at "Defence Space 2020", 17 November 2020, https://www.airpower.org.uk/defence-space-2020/

42 Timothy Thomas, "Russian Combat Capabilities for 2020: Three Developments to Track", Mitre Corporation, December 2019, https://www.armyupress.army.mil/Portals/7/Legacy-Articles/documents/Thomas-Russian-Combat-Capabilities.pdf

43 Clint Reach, "Review of Strategic Deterrence Book: The Work of Burenok and Pechatnov (2011)", Russia Strategic Initiative, HQ, USEUCOM, 3 December 2020.

communication systems, antennas, telecommunication towers, and associated support infrastructure. By default, contingency planning for civilian facilities of this kind will consider a number of risks such as fire, flood, or intrusion; but resilience to deliberate attack by a well-resourced hostile nation state would entail an entirely different order of security.

Where they exist, single points of failure will be particularly attractive to hostile actors. For several years, internet provision for the entire east of Latvia, including the Latgale region (briefly prominent as a candidate in widely discussed scenarios for a Russian intervention in the Baltic states), reportedly depended on cables under a single bridge across the Daugava river – in the same manner as Crimea's internet access could be controlled by physical intervention at a single point. The aim of this intervention may not be destruction; again, as in Crimea, physical presence inside a trusted facility opens a wide range of possibilities for controlling, selectively interdicting, or manipulating data – or indeed gaining easier remote access to other facilities by appearing to come from inside their security perimeter.

The need for close investigation of potential targets lies behind a sustained effort by Russia to covertly map the United States's telecommunications infrastructure and communications chokepoints,[44] in some instances in suspected coordination with reconnaissance flights carried out by Russian aircraft over the United States under the Open Skies Treaty.[45] In other cases, operations on land spill over from investigating subsea or space targets. Russia has sent covert intelligence officers to Ireland to map precise locations and vulnerabilities where submarine cables linking Europe and America make landfall.[46] Finland in particular has seen media reporting of alarm at the apparently systematic acquisition by Russian interests of land and properties in key locations near strategically important facilities, including "locations related to telecommunication links".[47] The Turku archipelago, in the narrowest stretch of water between southern Finland and Sweden, has been highlighted as a key location where communications cables, energy interconnectors, and strategically important sea lanes are vulnerable.[48] Speculation persists that Russian-owned properties in the

44 Ali Watkins, "Russia Escalates Spy Games after Years of US Neglect", *Politico*, 6 January 2017, https://www.politico.com/story/2017/06/01/russia-spies-espionage-trump-239003

45 Zach Dorfman, "The Secret History of the Russian Consulate in San Francisco", *Foreign Policy*, 14 December 2017, https://foreignpolicy.com/2017/12/14/the-secret-history-of-the-russian-consulate-in-san-francisco-putin-trump-spies-moscow/

46 John Mooney, "Russian Agents Plunge to New Ocean Depths in Ireland to Crack Transatlantic Cables", *Sunday Times*, 16 February 2020, https://www.thetimes.co.uk/past-six-days/2020-02-16/ireland/russian-agents-plunge-to-new-ocean-depths-in-ireland-to-crack-transatlantic-cables-fnqsmgncz

47 Ari Pesonen, "Tietoliikenneyhteyksien katkaiseminen olisi Venäjälle tehokasta sodankäyntiä" (Disconnecting telecommunications would be an effective form of warfare for Russia), *Uusi Suomi*, 27 October 2015, http://aripesonen1.puheenvuoro.uusisuomi.fi/205516-tietoliikenneyhteyksien-katkaiseminen-olisi-venajalle-tehokasta-sodankayntia

48 "Suomen vesiväylät 'motissa' – venäläisfirma osti maat" (Finnish waterways 'in a motti' after Russian company buys land), *Iltalehti*, 19 January 2015, http://www.iltalehti.fi/uutiset/2015011919044524_uu.shtml; "Maakauppoja strategisissa kohteissa", *Iltalehti*, 12 March 2015, http://www.iltalehti.fi/uutiset/2015031119338528_uu.shtml

archipelago raided in a major operation by the Finnish Tax Police, Border Guard, and Defence Forces in late 2018 were intended for use in an interdiction operation as opposed to being simply a non-political money laundering enterprise.[49]

Information interdiction can also be brought about remotely, using Russia's extensive suite of EW capabilities, one of whose key tasks is to "counter the enemy's advantages in the information and telecommunications space".[50] Russia claims that its "Murmansk BN" system deployed on the Kola Peninsula can disrupt communications across northern Europe, with a range of up to 5,000 kilometres.[51] It should not be assumed that the targets for this disruption will be wholly, or even primarily, military: while EW is supposed to achieve the military aims of "delaying timely information support to decision-makers, misguiding them with false information, constructing information blockades, warping databases, and destruction",[52] Russian military thought leaders have also predicted that in the initial period of war, the EW Troops will be tasked with suppressing broadcast and online media, including social media – specifically "blocking radio and television signals, and message traffic in social networks".[53] Russia's capabilities may in fact match its ambition of effecting information interdiction at all levels from individual connected devices such as mobile phones[54] up to national level, affecting broad-scale geographic areas and entities.[55] Both the intent and the capability, and the spillover from military aims to civilian consequences, have been demonstrated by Russia's repeated disruption of GPS navigation provision.[56]

49 Robin Häggblom, "A Dawn Raid in the Archipelago", Corporal Frisk blog, 23 September 2018, https://corporalfrisk.com/tag/airiston-helmi/; see also Joseph Trevithick, "Rumors of Covert Russian Ops Swirl After Finland's Police Raid Bond-Esque Private Island", *The Drive*, 1 November 2018, https://www.thedrive.com/the-war-zone/24616/rumors-of-covert-russian-ops-swirl-after-finlands-police-raid-bond-esque-private-island

50 Yuriy Lastochkin, "Солдаты РЭБ на страже эфира" (EW Troops guarding the airwaves), *Krasnaya Zvezda*, 15 April 2019, http://redstar.ru/wp-content/uploads/2019/04/041-15-04-2019.pdf

51 Jarmo Huhtanen, "Venäjä julkaisi videon, jossa harjoiteltiin häirintä¬järjestelmän käyttöä lähellä Suomen rajaa" (Russia releases video showing training with jamming system near Finnish border), *Helsingin Sanomat*, 13 November 2020, https://www.hs.fi/kotimaa/art-2000007615087.html

52 I. I. Korolyov et al., "Problems in Determining the Methods for Using the Forces and Means of Radio Electronic Warfare as an Arm of the Ground Forces", *Voennaya Mysl*' (Military Thought), No. 9, 2016, pp. 14–17.

53 S. G. Chekinov and S. A. Bogdanov, "Прогнозирование характера и содержания войн будущего: проблемы и суждения" (Forecasting the nature and content of wars of the future: problems and assessments), *Voennaya Mysl*' (Military Thought), No. 10, 2015, pp. 44–45.

54 Kelsey D. Atherton, "Russian Drones Can Jam Cellphones 60 Miles Away", C4ISRNET, November 2018, https://www.c4isrnet.com/newsletters/unmanned-systems/2018/11/16/russian-drones-can-jam-cell-phones-60-miles-away/

55 Martti J. Kari, *Russian Strategic Culture in Cyberspace: Theory of Strategic Culture*, JYU Dissertations 122 (Jyväskylä, Finland: Faculty of Information Technology, University of Jyväskylä, October 2019), 61–63, https://jyx.jyu.fi/bitstream/handle/123456789/65402/978-951-39-7837-2_vaitos_2019_10_11_jyx.pdf

56 Aleksandr Gostev, "'Мишки' на Севере. Был ли российский спецназ на Шпицбергене" ("Little bears" in the north. Was there a Russian Spetsnaz force on Spitsbergen?), Radio Svoboda (Radio Liberty), 2 October 2019, https://www.svoboda.org/a/30195704.html; Kyle Mizokami, "Russia Is Disrupting GPS Signals and It's Spilling into Israel", *Popular Mechanics*, 1 July 2019, https://www.popularmechanics.com/military/weapons/a28250133/russia-gps-signals-israel/

Disruption of GPS has a clear military application in preventing the use of those Western military systems that depend on it for navigation or guidance. But widespread and intensive use of this tactic would also cause severe societal disruption whether within or without an overt conflict due to ubiquitous reliance on positioning, navigation, and timing (PNT) services and the atrophy of skills and services that would replace them.[57] Road movements and every other type of activity that depends on GPS would be hampered; navigation systems without multiple redundancies and fallback systems would be affected, as would millions of embedded systems. Military movements would be impacted even if military navigational systems themselves were resilient; with civilian traffic reliant on GPS, chaos on road networks would be likely. Similarly, in the air, while commercial air traffic would continue to be able to navigate due to redundancy of systems, general aviation with greater reliance on GPS would cause severe ATC and traffic management challenges, for instance by blundering into busy controlled airspace.[58]

D. Online

Finally, adversaries still have the option of destructive effects delivered against information resources remotely through exclusively cyber means. A survey of Chinese cyber activity in the first decade of this century, in addition to intelligence-gathering, identified a range of "activities designed to damage or destroy network elements... as well as infrastructure dependent on those elements, such as communications systems".[59] Continuing concerns over potential hidden payloads in Chinese software, hardware, and firmware drive ongoing debate on the impact on network security of reliance on Chinese providers such as Huawei.[60]

Russia, meanwhile, has developed other means of denying access to the internet for ordinary users, including through exploits such as the VPNFilter malware, capable of permanently disabling home and small office internet connections on demand.[61] Russia's attack on the French TV channel TV5Monde in 2015 included erasing the firmware on nearly all of the network's routers and switches, resulting in blank screens for viewers. A French government investigation concluded that the attackers' primary goal was destruction of the network (and thus its capability to broadcast).[62]

57 As highlighted by Gen. Sir Patrick Sanders of UK Strategic Command, speaking at "Defence Space 2020", 17 November 2020, https://www.airpower.org.uk/defence-space-2020/

58 See further discussion in Keir Giles, "Missiles Are Not the Only Threat", in *Beyond Bursting Bubbles – Understanding the Full Spectrum of the Russian A2/AD Threat and Identifying Strategies for Counteraction*, FOI, July 2020, https://www.researchgate.net/publication/342643740_Missiles_Are_Not_the_Only_Threat

59 Desmond Ball, "China's Cyber Warfare Capabilities", Security Challenges, 2011, pp. 81–103, https://www.jstor.org/stable/26461991

60 "The Security of 5G", House of Commons Defence Committee, Second Report of Session 2019–21 HC 201, https://committees.parliament.uk/publications/2877/documents/27899/default/

61 Liam Tung, "FBI to All Router Users: Reboot Now to Neuter Russia's VPNFilter Malware", *ZDNet*, 29 May 2018, https://www.zdnet.com/article/fbi-to-all-router-users-reboot-now-to-neuter-russias-vpnfilter-malware/

62 Matthew J. Schwartz, "French Officials Detail 'Fancy Bear' Hack of TV5Monde", *Bank Info Security*, 12 June 2017, https://www.bankinfosecurity.com/french-officials-detail-fancy-bear-hack-tv5monde-a-9983

This may have formed part of the testing of information warfare capabilities that Russia appeared to be engaged in during the period following Crimea, with the same aim of eliminating competing sources of information – and ensuring that just as in Crimea, governments are unable to communicate with their citizens and populations are denied access to outside information.[63]

3. IMPLICATIONS AND RECOMMENDATIONS

Information warfare in the holistic sense espoused by China and Russia extends far beyond the Western concept of "cyber" activities. As with so many aspects of this challenge, the first and most important task for defenders is recognising the nature and scope of the threat. While many other aspects of information warfare as practiced by adversaries are now much more clearly understood – for instance, the destructive power of disinformation – there has been little public recognition by NATO nations of their adversaries' ambition to deny them use of the internet through physical intervention. Ciaran Martin, formerly founding Chief Executive of the UK's National Cyber Security Centre, classes "adversarial infrastructure destruction" as Level 2 in an ascending five-tier classification of cyber capabilities. But this destruction refers to "persistent engagement" or "counter-cyber" activities delivered through cyberspace and intended specifically to degrade the adversary's cyber capabilities, as opposed to physical activity with broader objectives. Meanwhile, the same classification refers to "kinetic" attacks as Level 4; but here too the discussion is of disruption achieved through cyber rather than physical means. (This classification, interestingly, groups the TV5Monde attack discussed above under "kinetic" impact.)[64]

Once recognition of the specific nature of this challenge is assured, many other countermeasures are familiar from more traditional cybersecurity practice. Given the extent to which the potential targets are in private ownership, defence and security agencies need to foster even closer partnerships with industry in order to access its expertise and secure cooperation at critical moments.[65] Infrastructure owners will be needed to advise on the precise cause of outages in order to inform appropriate responses – to take an example from late November 2019, whether a major outage of e-government services is the result of a cyber attack by a hostile power, or of rats chewing through cables.[66]

63 See extensive discussion of this testing in Keir Giles, "The Next Phase of Russian Information Warfare", NATO Strategic Communications Centre of Excellence, November 2015, https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles

64 Ciaran Martin, "Cyber-Weapons Are Called Viruses for a Reason: Statecraft and Security in the Digital Age", King's College London, 10 November 2020, https://s26304.pcdn.co/wp-content/uploads/Cyber-weapons-are-called-viruses-for-a-reason-v2-1.pdf

65 Elisabeth Braw, "National Business Corps to the Rescue", *Foreign Policy*, 23 November 2020, https://foreignpolicy.com/2020/11/23/national-business-corps-to-the-rescue/

66 "E-services Inaccessible After Rats Chew through Wires", ERR, 21 November 2019, https://news.err.ee/1005241/e-services-inaccessible-after-rats-chew-through-wires

Industry can also assist governments with situational awareness in general. Preparations for many of the attack scenarios described above have protracted timelines. For destructive cyber attacks, preemptive establishment of persistent access to high-value digital and computerised targets can take place long in advance.[67] In space, similarly, "properly positioning an orbital weapon into an appropriate attack position will often take days or weeks".[68] If industry is maintaining an appropriate level of situational awareness, these preparations provide potential opportunities to detect suspicious activity and prepare countermeasures.

Education in awareness of the threat would involve building on current efforts at warning information consumers against disinformation, by informing civilian populations of situations where they may also be receiving apparently trustworthy communications from known sources, including their governments, that are tainted or manipulated as a result of foreign intervention. False messaging on a mass scale, including from previously trusted sources, should be prepared for. Citizens will in many cases find it easier to determine the authenticity of broadcast media than of online information; other NATO nations should consider emulating Latvia, which encourages the public to seek information in time of crisis from television or radio, rather than the internet.[69]

In addition to previous statements by NATO and member states on responses to cyber attacks, declaratory policy should include emphasis that an attack (whether "armed" or not) on critical information and telecommunications assets supporting NATO states would be regarded as a use of force against those states and incur costs accordingly. The ability and will to employ countermeasures against kinetic and non-kinetic attacks should be shown, following the example of French Defence Minister Florence Parly, who in July 2019 promised responses in kind to threats to French space assets.[70]

Meanwhile, the scope for constraint on dangerous activity in or against space through new international agreements seems limited. The rapid development of Russia's capabilities in this field, and its possible advantages over competitors, could account for Russia's position in the United Nations changing over the past decade from proposing arms control treaties in space[71] to opposing a UK initiative on "reducing space threats

67 See discussion in "Bearing Witness: Uncovering the Logic behind Russian Military Cyber Operations", Booz Allen Hamilton, 2020.

68 Rebecca Reesman and James R. Wilson, "The Physics of Space War: How Orbital Dynamics Constrains Space-to-Space Engagements", Center for Space Policy and Strategy, October 2020, p. 20, https://aerospace.org/sites/default/files/2020-10/Reesman_PhysicsWarSpace_20201001.pdf

69 Public information video from Latvian State Fire and Rescue Service, 9 May 2019, available at https://twitter.com/ugunsdzeseji/status/1126435222759800833

70 "France to Develop Anti-Satellite Laser Weapons: Minister", *France 24*, 25 July 2019, https://www.france24.com/en/20190725-france-develop-anti-satellite-laser-weapons-minister

71 "Proposed Prevention of an Arms Race in Space (PAROS) Treaty", Nuclear Threat Initiative, 23 April 2020, https://www.nti.org/learn/treaties-and-regimes/proposed-prevention-arms-race-space-paros-treaty/

through norms, rules and principles of responsible behaviours".[72] Furthermore, any meaningful conversation about the future of outer space would require buy-in from all parties involved – including China.[73]

In fact, adversaries willing to target internet infrastructure enjoy a substantial deterrent advantage, as a threat to sow financial or societal chaos through severing undersea cables or jamming GPS might cause a NATO nation to think twice before risking escalation of a confrontation.[74] At first sight, destructive activities against cyberspace might seem self-defeating, since destruction removes access for both the defender and attacker; furthermore, few countries in the world would be immune from the economic repercussions stemming from the impact of such an attack on a major Western power.[75] However, in this respect as in others, Russia has undertaken preparations in the form of efforts to isolate itself from the global internet in time of crisis, with resulting insulation from the blowback effects of any irresponsible activity Moscow might consider undertaking elsewhere.[76]

Instead, more visible deterrence by denial should also form a key part of mitigation strategy for NATO nations. As with all effective means of deterrence, none of the options is cheap or easy; but all are far cheaper and easier than a failure to deter the adversary. Reducing the incentives to target infrastructure could be achieved by demonstrating resilience and redundancy, including publicly developing the capability to operate with a degraded communications environment, which would reduce the perceived benefits of escalation into attacks on civilian systems. Additional measures to improve resilience could include:

- Solutions (albeit expensive and long-term ones) for space vulnerabilities, such as hardening satellites against directed energy attacks and dispensing decoys to confuse direct ascent ASATs.[77]

72 Elena Chernenko, "Звездные войны. Эпизод ООН: Скрытая угроза" (Star Wars: UN episode. The hidden threat), *Kommersant*, 10 November 2020, https://www.kommersant.ru/amp/4565504; "Sending 14 Drafts to General Assembly, First Committee Defeats Motion Questioning Its Competence to Approve One Aimed at Tackling Outer Space Threats", United Nations, 6 November 2020, https://www.un.org/press/en/2020/gadis3658.doc.htm

73 Beyza Unal and Mathieu Boulègue, "Russia's Behaviour Risks Weaponizing Outer Space", Chatham House, 27 July 2020, https://www.chathamhouse.org/2020/07/russias-behaviour-risks-weaponizing-outer-space

74 Katarzyna Zysk, quoted in James Glanz and Thomas Nilsen, "A Deep-Diving Sub. A Deadly Fire. And Russia's Secret Undersea Agenda". *New York Times*, 20 April 2020, https://www.nytimes.com/2020/04/20/world/europe/russian-submarine-fire-losharik.html

75 Louise Matsakis, "What Would Really Happen If Russia Attacked Undersea Internet Cables", *Wired*, 5 January 2018. https://www.wired.com/story/russia-undersea-internet-cables/

76 Juha Kukkola, "Digital Soviet Union", Research Publications No. 40, Finnish National Defence University, 2020.

77 Marcus Weisgerber, "US Air Force Looks For New Ways to Buy, Protect Satellites", *Defense One*, 5 February 2018, http://www.defenseone.com/business/2018/02/us-air-force-looks-new-ways-buy-protect-satellites/145745/

- Ensuring that new communications architectures include redundancies through multiple channels: fibre and cable landlines, mobile networks, and backup and relay stations, including potentially using unmanned aircraft to relay communications.[78]
- Doctrinal and behavioural innovations to reduce reliance on always-on connectivity. Alongside the teaching of media consumer skills in response to disinformation attacks, continuing essential functions by other means when internet access is disrupted or absent should form part of education.
- Preparation and practice by Western governments, and their armed forces, to operate in an environment where communications services normally taken for granted are unavailable. This must include provision and regular exercise of alternative means for distributing public information.
- Explicit inclusion in security and business continuity specifications for critical communications infrastructure of consideration of serious physical attacks – whether carried out by a disaffected conspiracy theorist as in the example that opened this paper, or by an adversary nation state.

Finally, where it is not already the case, both before and during a crisis, civilian internet infrastructure must be accorded the same degree of physical protection as other strategically important assets.

4. CONCLUSION

China, Russia, and other states have developed capabilities which could potentially disrupt or eliminate internet access for NATO states through direct or indirect action against civilian telecommunications infrastructure. Military operations since 2014 demonstrate the availability of telecommunications expertise to Russian special forces in particular, and point to an entirely new integration between cyber, information, and kinetic operations.[79] In effect, the asymmetric information warfare capabilities the Russian Armed Forces aspired to at the beginning of the last decade are now not only available but routinely put to use.[80]

It follows that in time of conflict, declared or undeclared, NATO states may find that access to internet resources may be degraded or entirely absent – including for the

78 Donna Attick, "Robust Communications Relay with Distributed Airborne Reliable Wide-Area Interoperable Network (DARWIN) for Manned-Unmanned Teaming in a Spectrum Denied Environment", Navy SBIR, January 2018, http://www.navysbir.com/n18_1/N181-007.htm

79 Sydney J. Freedberg, "Army Fights Culture Gap Between Cyber & Ops: 'Dolphin Speak'", *Breaking Defense*, 10 November 2015, http://breakingdefense.com/2015/11/army-fights-culture-gap-between-cyber-ops-dolphin-speak/

80 Compare Keir Giles, "Information Troops – A Russian Cyber Command?", Proceedings of the Third International Conference on Cyber Conflict, Tallinn, June 2011, https://www.ccdcoe.org/uploads/2018/10/InformationTroopsARussianCyberCommand-Giles.pdf, with discussion of Russian information activities in Syria in Tim Ripley, *Operation Aleppo: Russia's War in Syria* (Telic-Herrick Publications, 2018), p. 192 and passim.

purposes of communicating with their own civilian populations or Armed Forces personnel outside hardened and discrete networks. This applies in equal measure to using any other friendly capabilities which may be compromised by lack of access to the electromagnetic spectrum, including GPS signals. It is essential that conflict and crisis planning by NATO member states recognise this risk and take steps to mitigate it.