Booz | Allen | Hamilton®

2020 CYBERSECURITY THREAT TRENDS OUTLOOK

Nine ways threat actors will make waves in 2020

[1]This report is for informational purposes only, and Booz Allen makes no promises or warranties regarding the content, its accuracy, or your reliance on information contained herein.

The expectations for the year 2020 are massive, as major world events underscore mounting geopolitical tensions. The United States will elect a president, Tokyo will host the Olympics, and renewable energy is anticipated to outcompete fossil fuels. Likewise, this time of economic uncertainty and increased competition across industry is contributing to the rise of digital transformation. Unprecedented innovations have been promised to us. Commercial space programs will take us to Mars, we will control devices with microchips implanted in our brains, and cars will be fully autonomous. Whether the above will come to fruition, one thing is for certain: the transformational benefits of next-generation technology are here.

Leaders are investing in digital transformation to increase competitive advantages, drive operational efficiencies, and grow market share. Leading-edge technology companies are manufacturing products faster, advancing logistics processes, and filling talent gaps. Alongside this rapidly scaling digitalization is organizational convergence. Enterprises are aggressively expanding through mergers and acquisitions, and evolving across geographical markets and industry. All the while, threat actors continue to challenge innovative security systems, uncovering gaps and slipping into the globally connected landscape the world is constructing. Organizations that prepare for uncertainty and approach their digital transformation with a security-focused mindset will be better positioned to survive this increasingly hostile connected ecosystem. Today's leaders must approach their security challenges with the same imagination, agility, and tenacity as their adversaries.

This report not only captures what we are seeing across a complex cyber landscape but also identifies the necessary actions to remain resilient to continuously evolving threats and leverage security as a business enabler.

2019 PREDICTIONS THAT HIT THEIR MARK

Anticipating that the most advanced threat actors would seek to leverage the expanding ecosystem of Internet of Things (IoT) devices found throughout targeted environments, our analysts anticipated that state-sponsored adversaries would train their sights on IoT to be leveraged in espionage operations. In August 2019, researchers reported that Russia-aligned threat group APT28 had pivoted from compromised devices—including a Voice over Internet Protocol phone, printer, and video decoder—to establish a foothold on corporate networks.[1] **(IoT, State-Sponsored Threats)**

In addition to state-sponsored espionage, criminals have expanded their abuse of IoT. Booz Allen predicted that threat actors would rely on IoT proxy botnets to conceal their malicious activity, and between Q1 2019 and Q2 2019 attack traffic routed through residential IP addresses in the U.S.—including IoT devices—nearly quadrupled for the retail and financial services sectors.[2] Further, in June 2019, the U.S. Federal Bureau of Investigation reiterated the importance of securing IoT devices, in response to a surge of activity using these systems to proxy malicious traffic.[3] **(IoT, Criminal Threats)**

While 2019 did not see the rise of deep-fake video content in state-backed information operations, the first instance of cybercriminals using deep fakes has been observed. In at least one case in March 2019 that targeted a United Kingdom-energy firm, criminals used artificial intelligence-based software to impersonate the CEO's voice in phone calls requesting fraudulent fund transfers.[4]

As public utilities become a primary target for cyber attacks as interstate tensions rise, we predicted that critical infrastructure providing public water services would be targeted by nation-state threat actors. In August 2019, U.S. media reported that Iranian-sponsored hackers breached the network of Bahrain's Electricity and Water Authority, prompting the organization to take its systems offline.[5] **(Water Utilities, State-Sponsored Threats)**

Booz Allen predicted that threat actors would target proprietary wireless protocols in attacks against enterprise networks. Though in-the-wild attacks remain just over the horizon, new attack vectors for proprietary wireless protocols continue to be revealed. In July 2019, researchers detailed several vulnerabilities in Logitech's "Unifying" protocol—used for wireless mice and keyboards—that could be exploited to allow an attacker to capture keystrokes and mouse actions transmitted over the protocol and inject arbitrary actions.[6]

Regional internet and technology industries are increasingly divorced and isolated; organizations will struggle to secure data and the integrity of their systems and networks across the new digital sovereign divide.

To be successful in this new age of technological division, organizations must understand new national and local laws governing use of technology and the internet, understand and employ national and local technologies to remain competitive, but at the same time be careful of introducing tech with limited vetting into corporate networks.

GLOBAL BALKANIZATION OF TECHNOLOGY

BALKANIZATION OF TECHNOLOGY

As global technology advances, political actors and governing institutions both national and international are struggling mightily to keep pace with their policymaking. While some governments have embraced a laissez-faire attitude, other governments on the international stage are adopting a more hands-on approach. Different styles of governance have contributed to a rift in the technology sector and in fact challenge the core idea of the globally connected internet. Disparate operating systems for computers and mobile devices, next-generation networking infrastructure, and Balkanized internet will create entirely different digital environments for organizations within the next several years.

SEEKING INTERNET HEGEMONY

In February 2019, Russia announced it was again preparing to isolate itself from the global internet in case of cyber attacks against the country.[7] And in May of 2019, President Putin signed into law a bill requiring Russian internet service providers to filter all internet traffic through the Kremlin's Roscomnadzor internet censor node, in hopes of creating a "RuNet."[8] Moscow has also pressed to develop independent network infrastructure for BRICS nations (Brazil, Russia, India, China, South Africa) and create a separate Domain Name System.[9] Russia's attempts to develop a sovereign network since at least 2014 have precipitated a notable trend of 'Balkanization' of networks and technologies across the globe.

China, meanwhile, wants to become a leader on internet policy as it cultivates relationships in Asia and the Middle East.[10] At least 30 countries have received China's media and information management training.[11] In Vietnam, for example, this training likely led to the passage of a surveillance and anti-privacy law like its Chinese counterpart in 2018.[12] Beijing will very likely continue to strengthen its Great Firewall while also building a bloc of like-minded nations that support its segmentation efforts. Recent geopolitical upheaval like the persistent anti-extradition protests in Hong Kong[13] would be easily quelled if China effectively controlled web traffic in and out of East Asia.

POLICY VS. TECHNOLOGY

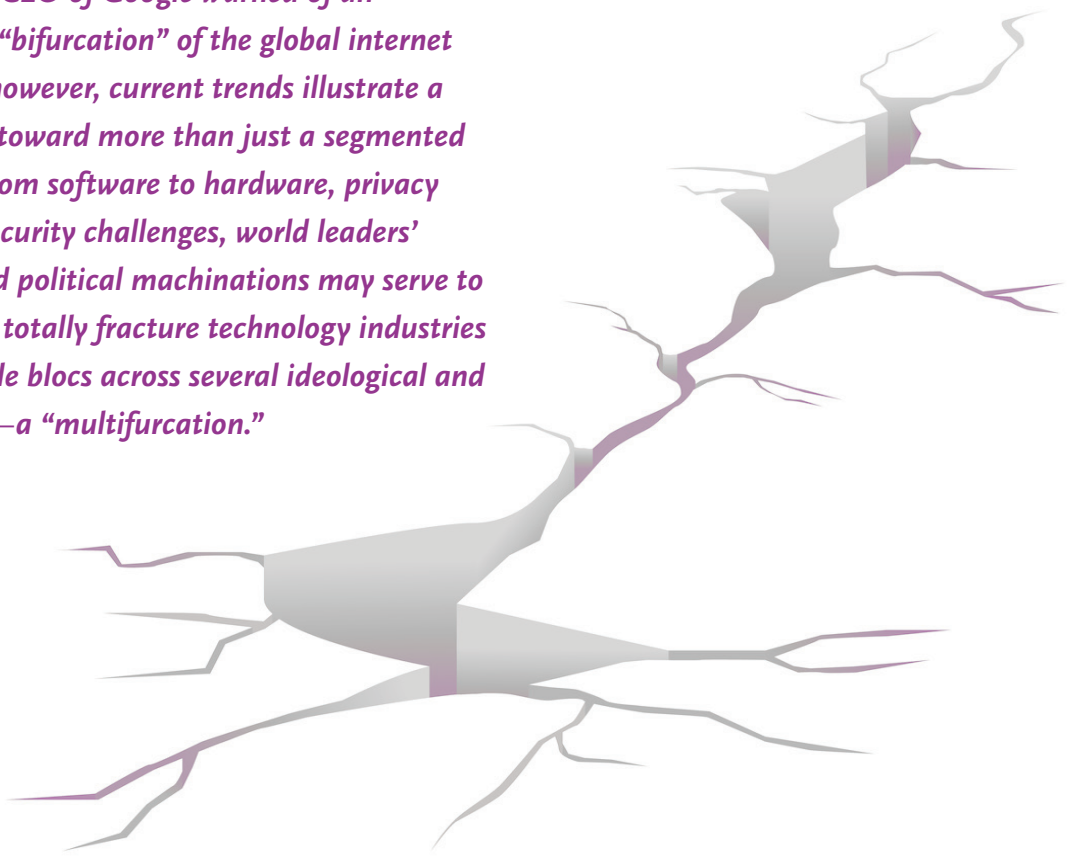
The blame for this modern technological Balkanization cannot be laid only at the feet of Russia and China; Western countries like the U.S. have played their part as well. Huawei has developed a line of 5G devices and infrastructure technologies at competitive price points, but these options have been snubbed by the U.S. and U.K. governments;[14] Western banning and blacklisting of Huawei products have been motivated by both ethical and geopolitical concerns.[15] Unfortunately, as Western technology and internet companies expand globally, they may avoid certain markets altogether, because of certain restrictions or laws in the host country. For example, Google recently terminated a plan to launch a censored search engine in China,[16] thus leaving room for national and regional alternatives in the local market and further sharpening the digital sovereign divide between East and West.

THE DEMISE OF STANDARDIZATION

Network segmentation is not the only issue threatening to contribute to today's Balkanization of tech. A look at market shares for mobile operating systems reveals just how reliant the tech world is on Western operating systems like Google's Android and Microsoft Windows. These giants of the software industry have a virtual stranglehold in their respective markets: As of June 2019, Android had a 76% global market share;[17] in Asia, Android held an even more commanding 84% share of mobile operating systems.[18] Windows fares similarly well, jumping from 78% globally to 81% share in Asia.[19]

Having recognized its reliance on Western software, and in the wake of rising tensions between the U.S. and Huawei, the Chinese tech company has been developing an alternative to the Android operating system.[20] Though the U.S. recently signaled the ban preventing the sale of American tech to Huawei may end soon,[21] Huawei will likely remain motivated to develop an alternative to help alleviate the pain of potential future sanctions.

The former CEO of Google warned of an impending "bifurcation" of the global internet by 2028;[22] however, current trends illustrate a movement toward more than just a segmented internet. From software to hardware, privacy norms to security challenges, world leaders' cultural and political machinations may serve to partially or totally fracture technology industries into multiple blocs across several ideological and state lines—a "multifurcation."



As battle lines are drawn between geopolitical adversaries, consumers and corporations alike may be caught in the crossfire.

Surprisingly, technology Balkanization may be beneficial in some ways: for example, malware developed to target machines running Huawei's future operating system may not operate on Windows machines or on Android phones. But overall the result of this digital divide will likely be predominantly negative. Companies and consumers in some areas will struggle or perhaps be unable to secure their data, as they suffer draconian espionage and censorship laws. Local and regional operating systems and other software will lack the complex and effective infrastructure for malware detection, information sharing, and patching that companies and individuals have relied upon in the past.

What you can do to mitigate this threat:

Businesses must adapt to this new multipolar world of technology. Some recommendations for organizations and their leadership teams are to:

- Build leadership proficiency in navigating complex and varied regional and local laws governing technologies, privacy, and connectivity to the global internet.
- Motivate personnel firmwide to research, understand, and employ regional and local technologies that are required for operation in certain areas.
- Use caution when integrating software or hardware with limited vetting into the organization's networks, and segment networks to minimize exposure from potentially vulnerable hardware or software.

Rising demand for electronic components will expand the market for counterfeit components and cloned products, subsequently increasing the threat of compromised hardware finding its way into organizations' supply chains.

Global production of electronic devices is growing rapidly, driving demand for replacement parts and new components.

Scarcity of resources strains supply chains, creating opportunities for counterfeit components to enter the manufacturing process and providing threat actors opportunities to distribute malicious hardware.

Remediation is likely best accomplished through preventative measures, such as monitoring throughout the supply chain and inspection of components and devices for tell-tale signs of tampering or counterfeiting.

TAINTED COMPONENT: CLONES AND COUNTERFEITS

EXPANDING OPPORTUNITIES FOR HARDWARE SUPPLY-CHAIN ATTACKS

The supply chain for computer systems is deep, rife with third-party suppliers, hardware vendors, coders, and facilities across multiple countries and continents charged with shipping, manufacturing, assembling, and customizing computer systems.[23] This depth complicates supply chain quality control and provides opportunity for threat actors to introduce compromised hardware. In recent years, prominent reporting has cried wolf with allegations of state-backed espionage via malicious chips inserted during manufacturing of critical IT systems[24] —claims that were widely met with denials.[25] However, the vectors for hardware supply-chain attacks are expanding as market demand for more and cheaper chips and components drives a booming business for hardware counterfeiters and cloners. This expansion is likely to create greater opportunity for compromise by both nation state and cybercriminal threat actors.

CLONES AND COUNTERFEITS

Counterfeit Components

During the manufacturing process, critical components such as organic light-emitting diode displays, dynamic random-access memory, and NOT-AND (NAND) can be rapidly consumed, leading to supply shortages.[26] To meet deadlines and compressed timetables, companies facing minimal scrutiny in quality control may choose to purchase unverified components and risk introducing counterfeit chips. Similarly, repairing legacy systems well past obsolescence may require components that are no longer in production, forcing reliance on alternative suppliers. This is a significant challenge for the military and other organizations that use systems that have been in operation for decades. Dilemmas such as these create demand for a counterfeit chip market. With counterfeit chips, previously used circuit boards are stripped of their components, and the parts are polished, tinned, and refurbished to appear new. In 2007, the U.S. Federal Bureau of Investigation identified counterfeit electronic components as 900% more profitable than cocaine distribution.[27]

In multiple instances, counterfeit mislabeled non-military grade chips made their way onto weapon systems, including aircraft, ships, submarines, and missile defense systems.[28] The chips are often salvaged overseas, but domestic firms have been cited for illegally procuring the chips and marketing them as new.[29] Counterfeit components have also compromised consumer devices, including insertion of chips designed to introduce malicious code, vulnerabilities, or failure into the system for malicious purposes. Examples of malicious implants have been observed in compromised smartphone screen replacement components, in which manufacturers have reportedly installed chips containing malicious code that ultimately allowed access to the mobile device.[30]

Cloned Electronics

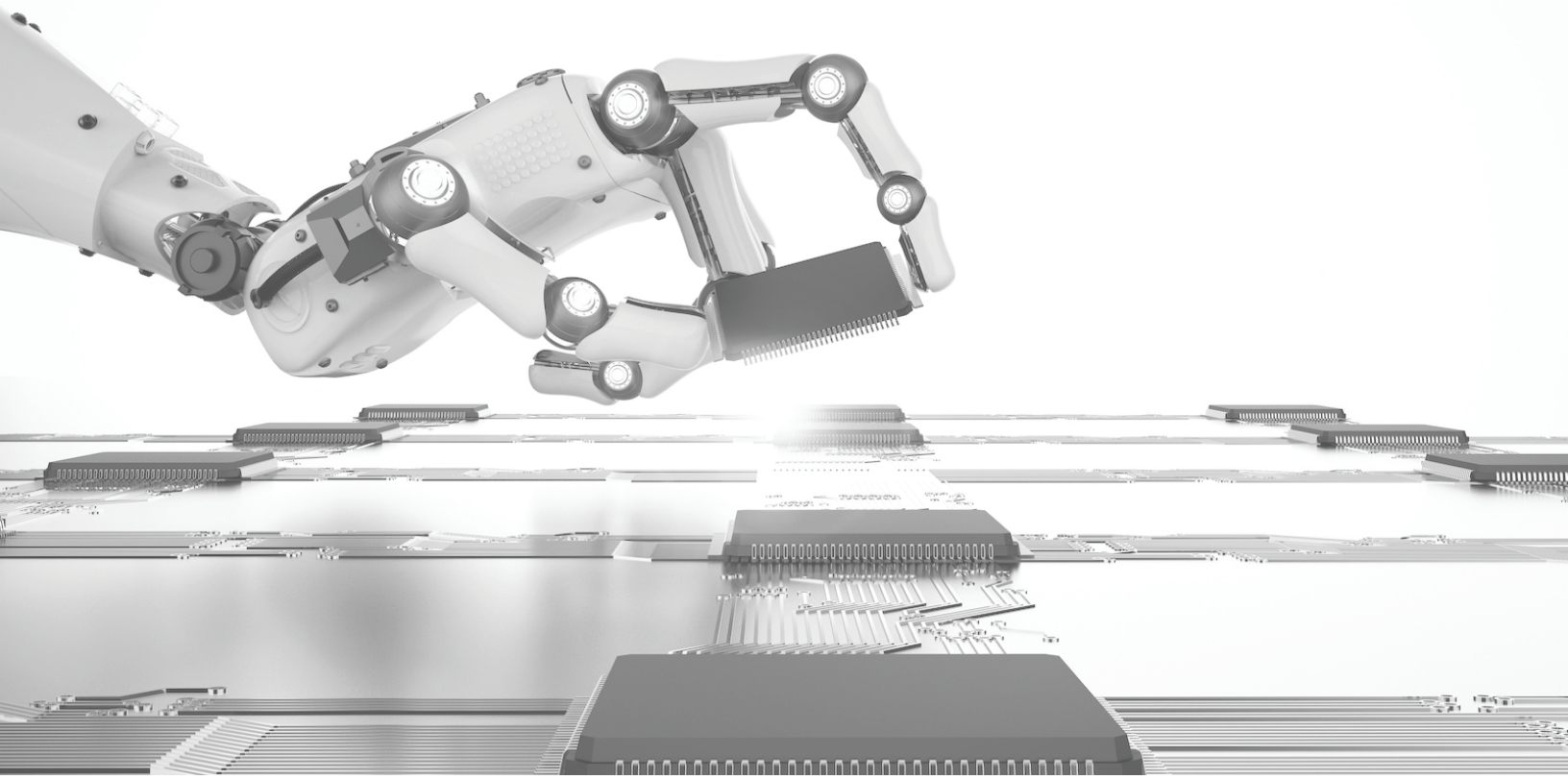
In addition to device components or chips, entire products designed to mimic trusted brands can be produced by unscrupulous manufacturers. Cloned electronics are devices that appear to be genuine but are the product of reverse engineering and unlicensed production, packaging, and resale.[31]

Device cloning is believed to be widespread and includes devices such as routers, switches, automotive monitoring equipment, among other systems.[32] Even high-end electronics, such as laptops, can be cloned and sold as real, forcing manufacturers to expend resources to ensure customers can identify forged products.[33] The prevalence of these products is due in part to complicated supply chains that make it difficult to distinguish between genuine products and cloned fakes,[34] and cloned devices can often be purchased through legitimate market places, such as popular online retailers, that grants added legitimacy.[35] The use of cloned electronics can pose significant safety concerns for users because the components are often substandard, damaged, or lack the durability required by the genuine product.[36] Common devices like cloned phone chargers have caught fire and failed safety testing, undercutting the reputation of the manufacturer of the copied products.

In 2007, the U.S. Federal Bureau of Investigation identified counterfeit electronic components as 900 percent more profitable than cocaine distribution.

INCREASED DEMAND AND INCREASED THREATS

Cloned or counterfeit components need not be a nation state-directed activity, because the market demand will likely provide profit-motive. The rapid rise in demand for consumer electronics, especially IoT devices, will overwhelmingly increase demand for electronic components. Simultaneously, this demand is likely to drive production of counterfeit or cloned components and devices, as consumers seek low-cost versions of otherwise premium-priced products. For years, North America accounted for the greatest demand for components because of a rise in demand for IoT devices—a trend expected to continue for years to come—though rising wages and spending in countries like China are also expected to expand the consumer market and further drive demand for electronic components.[37] In 2020, this demand will almost certainly push counterfeit component producers to redouble efforts in supplying counterfeit inventory to manufacturers, and improve processes to develop more convincing fakes. Cloned products may also be readily available, likely bypassing official vendors and retailers, to distribute products—ranging from enterprise routers to consumers products—via online markets.



What you can do to mitigate this threat:

Mitigations that may help organizations prevent or limit the impacts of compromised hardware components making their way into the supply chain include:

- Procurement channels should strictly detail their supply chain to ensure unknown or non-trusted vendors do not supply parts. [38]
- Finished products should be audited by a third party and inspected to ensure they meet the bill-of-material.
- Organizations may check for incorrect part numbers, date codes, country of origin markings, misspellings on logos, crooked type, non-machine typed lettering, and soldering marks on pins of new products; review can include comparing original-equipment-manufacturer components against new products for discrepancies. [39]
- Organizations may employ an engineer to oversee the manufacturing process at the factory. While this is sure to add cost, it can dissuade insiders from conducting illicit activity during production processes.
- Systems using system-on-a-chip (SoC) components should test factory firmware cross-reference with an accepted baseline.

The rapidly increasing body of data generated by automobiles—through both the integration of consumer applications and rollout of self-driving vehicles—is likely to drive cybercriminals to specialize in targeting vehicle-borne systems.

Automobiles are set to become massive sources of data, including operational data as well as consumer personally identifiable information (PII) and financial data.

Wide adoption of mobile phones has spurred criminals to specialize in targeting these platforms; this trend will likely be emulated with criminals and malware developers specializing in targeting automotive data, as the body of targetable data similarly grows.

Data will present multiple avenues for monetization, including theft of financial data or other PII from vehicle-based applications or real-time location monitoring to enable non-cyber criminal activity—such as theft or smuggling operations.

Mitigations may be split to harden vehicles themselves against attacks (for example securing hardware ports and consumer-facing wireless interfaces), as well as measures to secure backend databases holding vehicles' operational data and sensitive customer information.

CYBERCRIME HITS THE HIGHWAY

THE AUTOMOTIVE DATA DELUGE

Interference with critical sensors or unauthorized manipulation of vehicle controls has been top of mind for automotive companies, regulators, security researchers, and others concerned about the looming safety threat of cyber attacks on these systems. However, threats to consumers and vendors are not isolated to digital vehicle hijacking but extend to the massive trove of data that vehicle-borne systems produce. Vehicle-generated data may present a more readily monetizable target, and in turn, will likely be the primary focus of cybercriminal operations. In the near-term the array of consumer-facing, vehicle-borne software—from payment apps to in-vehicle entertainment systems—will likely represent the biggest target for threat actors seeking to steal customer PII for resale, identify fraud, or other traditional cybercriminal activity. More long term, as fleets of self-driving, autonomous vehicles (AV) are brought to market, the stream of data from sensors required to operate these AVs—as high as 4 terabytes for every 90 minutes of operation, according to at least one estimate[40]—may provide a window of opportunity for cyber-enabled crime, including theft or smuggling operations.

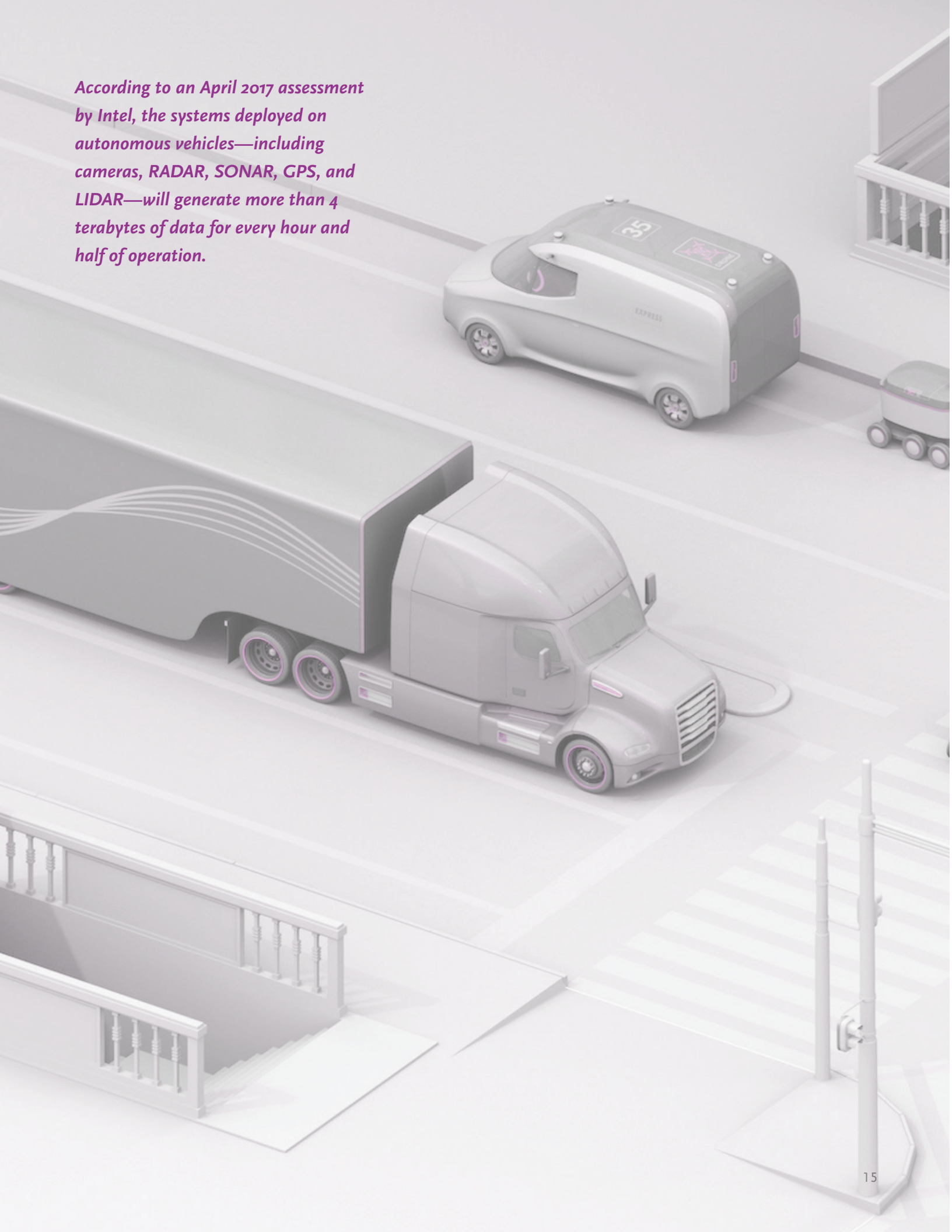
DRIVERS IN THE CROSSHAIRS: STEALING VEHICLE DATA

Researchers have demonstrated several ways in which vehicle-generated data can be exposed; their findings highlight that such data can be compromised through malicious targeting or vendor negligence and can be collected locally from the vehicles or remotely from the infrastructure managing the data. Researchers have shown an ability to field devices that track a car's location within a road network by monitoring the vehicle's Common Awareness Message and Basic Safety Message wireless messaging,[41] and a separate researcher discovered more than 540,000 customer records exposed by a vehicle tracking service provider on a misconfigured cloud storage server, including customer account credentials, vehicle information, and tracking data generated by global positioning system (GPS) devices on customer vehicles.[42]

MONETIZING VEHICLE DATA

With researchers demonstrating the availability of vehicle data, the remaining element to drive cybercriminals to focus on vehicle systems is proven methods to monetize stolen data and associated markets to resell it. As of 2019, the beginnings of these monetization methods have begun to emerge. In July 2019, researchers reported the sale of Mercedes Benz credentials on a cybercriminal forum,[43] including credentials for smartphone applications used to remotely monitor and access Mercedes vehicles, provide the ability to remotely locate, unlock, and start vehicles, among other functions.[44] In addition, efforts to abuse app-based remote vehicle access have already been used to enable real-world crime targeting connected cars. In early 2019, efforts to roll out a luxury car sharing service in Chicago resulted in widespread theft of the vehicles—many of which were dismantled for parts—by criminals that had furnished bogus accounts using fake or stolen credit card information.[45]

According to an April 2017 assessment by Intel, the systems deployed on autonomous vehicles—including cameras, RADAR, SONAR, GPS, and LIDAR—will generate more than 4 terabytes of data for every hour and half of operation.



VEHICLE THREATS ON THE HORIZON

Cybercrime targeting connected vehicles in the short term is likely to look much the same as other cybercrime observed to date. Account credentials, PII, and payment data that can be recovered from onboard software will likely be the first targets. For example, as manufacturers begin to integrate cashless payment applications directly into vehicle-based systems,[46] such apps are likely to be a major interest for cybercriminals—stolen payment data would be most easily resold in existing cybercriminal marketplaces. While malware impacting vehicle systems have been found in the wild—including "Mirai Okiru" a malware designed to infect Argonaut RISC Core (ARC) CPUs, which are embedded in billions of system-on-a-chip devices including automotive systems—an expected development would be malware specifically targeting infotainment systems and consumer-facing software.[47] Similar to the flourishing mobile market that has popped up in criminal communities, specialized malware designed to steal customer data from vehicle-borne apps is likely to emerge.

In the midterm, as AVs become commonplace on the highway, cybercriminals are likely to target these systems as well. Widespread automation of long-haul trucking will likely be the tip of the spear for AV deployment—test trials for autonomous cargo trucks began as early as 2015[48] —and commercial AVs in remote locations may be ideal targets for criminals to monitor, intercept, and ultimately steal cargo or add contraband. Incidents in the commercial shipping sector highlight that the monitoring of navigation and safety broadcasts is a common practice for criminals, to the extent that the International Maritime Organization updated its guidance on system usage, advising operators to disable certain systems in high-risk areas.[49] As autonomous trucking becomes more widespread, interest among cybercriminals may increase in exploiting the corresponding technology—including wireless vehicle communications, or backend infrastructure detailing vehicle operations.

As threats to critical infrastructure paved the way for niche operational technology (OT)-focused cybersecurity offerings, the widespread adoption of AVs will likely spur the emergence of similar specialists seeking to address the unique challenges of securing and managing networks where the assets are geographically dispersed, mobile, and continuously generating troves of sensitive data.

What you can do to mitigate this threat:

- Manufacturers should address threats targeting customer data used in vehicle-borne apps. This includes hardening vehicles to prevent delivery of malware—for example securing hardware ports and wireless interfaces.
- Manufacturers should also consider segmenting onboard systems to prevent attacks targeting consumer software from impacting systems used for vehicle operation.
- Manufacturers should ensure security measures are implemented for customer data generated by vehicle-borne systems—a measure that would increasingly apply to operational data, as commercial AVs are deployed.

As drones evolve from novelty item to a ubiquitous business tool, resourceful network intruders may see an opportunity to leverage drones' proximity to homes and businesses to turn the machines into a jumping-off point to networks and systems, thus creating a new category of infection vector from which organizations must defend themselves—airborne malware and exploit delivery.

Drones are being leveraged in an increasingly wide range of industries and are becoming ubiquitous in the physical space in which people live and conduct business.

Researchers have demonstrated a range of network attacks using drones, which could allow threat actors to establish a network foothold, deliver malware, or otherwise interfere with wireless networks.

As threat actors adopt the use of drones as delivery mechanisms for targeted attacks, organizations may be forced to treat their airspace as an extension of their attack surface.

MALWARE TAKES FLIGHT: DRONES AS AN INITIAL NETWORK INFECTION VECTOR

DRONE ATTACKS NO LONGER A PLAYGROUND FOR RESEARCHERS

We are fast approaching a time when the sight of drones buzzing around our neighborhoods, office buildings, and other public spaces will be commonplace; an expected, sometimes unnoticed, element in the backdrop of our lives. Package and cargo delivery, security monitoring, building safety inspections, crop monitoring, and 3D mapping are just a few of the areas in which commercial drones are currently employed, and their use is expected to grow by a factor of 10 between 2016 and 2021.[50]

Drone-based network attacks are not unprecedented, but to date, the tactic has predominantly remained in the realm of controlled research environments. Security researchers have demonstrated drone-based attacks that range from the simplistic to the complex and esoteric. Drones hovering outside office windows have hijacked a Bluetooth mouse to silently install malware on a computer, and a drone-mounted video recorder was used to receive communications from a malware-infected computer that emitted light pulses through a window.[51] Still, the public availability of veritable "pentesting labs with wings" suggests that drone-based network intrusions may not remain solely in the domain of researchers.[52] Drones equipped with a Raspberry Pi and Kali Linux—a platform that includes hundreds of pentesting programs—can be purchased online, and freely available tutorials and attack drone design plans may significantly reduce the barriers to entry for drone-based network attacks.

The use of drones as rogue WiFi access points may be one of the most simplistic yet effective tactics for targeting individuals. Drones equipped with a device like a WiFi Pineapple can be placed in proximity to a targeted company and be used to harvest credentials, perform man-in-the-middle attacks, and conduct network reconnaissance. Even users connected to legitimate company access points could conceivably be forced to connect to the drone's WiFi if the target's network does not prevent forced deauthentications.[53] Drones may be parked on the roof of a building, in bushes, window ledges, and other concealed locations, including those that are in enclosed locations that are otherwise off limits to foot and vehicle traffic.

Drones equipped with specially fitted hardware and software may also be used to install malicious malware on systems or disrupt system's operations, particularly devices that are vulnerable to exploitation of wireless protocols like Bluetooth and ZigBee. Israeli security researchers demonstrated that a drone could be used to manipulate ZigBee-controlled lightbulbs (they made them blink SOS in Morse code) via the exploitation of a previously undisclosed vulnerability in the ZigBee protocol, in combination with uniquely developed attack on the lightbulbs' encryption.[54] IoT devices often use ZigBee, and the attack is indicative of the potential impact that drone-based network attacks could have on all types of IoT devices, including those that are critical to the manufacturing, health, and energy sectors, among others.

What you can do to mitigate this threat:

- Organizations may train personnel providing physical security to recognize drones as a potential threat.
- For small office/home office wireless networks, operators may consider mitigations commonly used to address wardriving attacks, such as turning off the wireless network when not in use, updating administrator passwords on routers regularly, and using security measures such as wireless traffic encryption and firewalls.[55]
- Organizations that consider themselves at high risk of drone-based attacks may want to consider employing counter-drone defense systems that jam, hijack, or otherwise disrupt the flight path of the machines.

EXPANDED ATTACK SURFACE

Drone-enabled network attacks will never reach the scale of traditional remote network attacks, but the possibility of their use may require companies to consider their airspace as another component of an attack surface that must be defended. When ubiquitous, high-profile vulnerabilities like BleedingBit and BlueBorne—both Bluetooth code execution vulnerabilities—are disclosed, companies may need to consider drones as a potential vector of exploitation, particularly for devices and systems that are near windows or are in open spaces. The requirement for both the attacker and the drone to be in proximity to a target (e.g., Bluetooth has an estimated maximum range of 300 feet) will limit the frequency with which drone-based attacks will be used, but the threat nonetheless remains real.

Threat actor groups will increasingly target organizations providing ground-based command and control (C2) to satellite constellations, as orbital technology becomes increasingly critical to global infrastructure.

Modern attacks on space organizations have leveraged traditional IT and human elements to bypass obscure communications technology.

Disruptions to satellite technology have clear potential to become high-impact, high-visibility disasters.

Satellite technology is already important to many kinds of modern technology and likely to become even more critical in the coming decade.

Satellite C2 facilities need to adopt the kinds of information security practices developed for industrial control system environments.

THE FUTURE OF SATELLITES FOR EARTH, SPACE, AND THE INTERNET

THE STATE OF SPACE

When the Galileo Global Navigation Satellite System went offline for 5 days in July 2019,[56] experts in the information security field judged that a cyber attack was unlikely in this specific case—but all too possible and potentially destructive.[57] Today, satellites provide critical communications infrastructure, not only to space programs[58] or the military but also to the civilian sector, including navigation, location, communication, and timekeeping.[59] The modern world relies on satellite constellations, and satellite constellations rely on ground-based C2 facilities to function properly. As was the case with the Galileo outage, a failure on the ground can take down an entire constellation, and with it the global technologies that depend on it.[60]

Because ground control systems are more accessible from the public internet and usually encompass the hardware, software, and knowledge necessary to interact with specific satellites, they present the most tempting targets to threat actors. A cyber attack on National Aeronautics and Space Administration (NASA) Jet Propulsion Laboratory discovered in April 2018 exposed another weakness in these systems: the difficulty of managing a civilian computer network with public information, shared scientific data, and sensitive OT all working together. The result is a pathway from the public internet to critical technologies that is not supposed to exist with proper network segmentation.

IMPENDING CONSTELLATION MULTIPLICATION

Global reliance on satellite communications (SATCOM) is likely to increase greatly in the coming decade. In addition to the European Union's current project to complete its Galileo constellation, multiple space agencies are planning ambitious new missions, private space companies are expanding their operations, and satellite-based consumer internet access is anticipated within the next decade.[64] All these changes will increase the attack surface for threat actors targeting space infrastructure. The stakes and incentive for state-sponsored threat-actor groups in particular will increase if satellite broadband gains popularity, if a new "space race" develops among space programs, or these threat actors perceive commercial space flights as worthwhile targets.

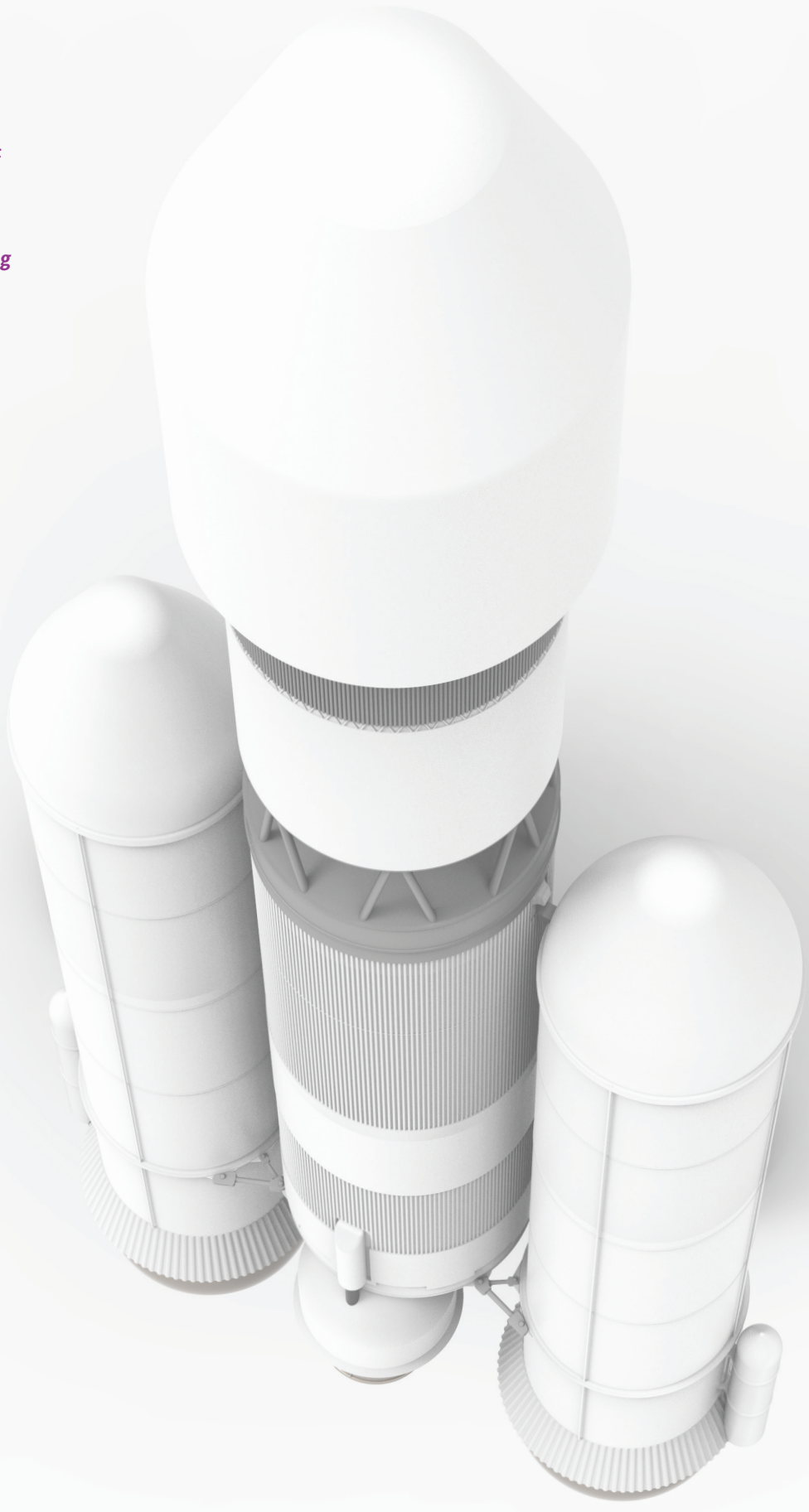
OBSCURE AND INSECURE SATELLITE COMMUNICATIONS

In-the-wild and proof-of-concept attacks serve to disprove a popular misconception that threat actors cannot attack satellites because the equipment is too specialized or restricted and the communications protocols too complex for an outsider to use. Frontal attacks on these specialized systems may be difficult, but tried and true methods involving email, exposed servers, and social engineering can bypass those protections, just as they do with typical commercial victims.

The April 2015 case of satellite television network TV5Monde illustrates how little satellite infrastructure can factor into an attack. In this scenario, APT28 gained initial access through compromised virtual private network credentials and used a combination of Active Directory tools and Remote Access Tools to pivot around the network and eventually corrupt most of the victim's network-connected systems.[65] The result was that TV5Monde's satellite television network went dark for months.[66] The attacker never needed to communicate directly with any satellite.

Security researchers have also demonstrated techniques for compromising multiple types of satellite-reliant communications technology, including on airplanes, boats, and military technology.[67] For the most part, these demonstrated attacks would pose little or no physical danger to the craft or the satellite systems. However, in the case of high-powered military SATCOM transponders, they have found that an attacker could increase power to the antenna, such that it could injure people or even damage electronics on the satellites themselves.[68] In scenarios like these, threat actors simply steal C2 resources from human victims or systems tasked with legitimately controlling satellite constellations, rather than trying to reverse engineer those resources.

A simple Shodan search returns thousands of NASA services publicly available online including File Transfer Protocol, Lightweight Directory Access Protocol, and Simple Mail Transfer Protocol.[61] *Services like these can provide footholds to threat actors targeting space C2 services in the U.S.,* [62] *France,*[63] *Norway, and beyond.*

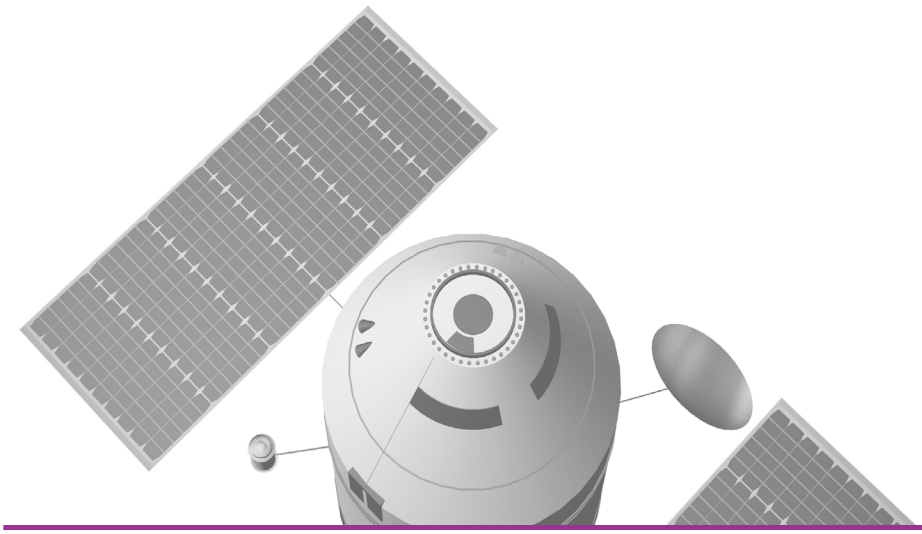


To better protect satellite infrastructure as it becomes more prolific and integrated into modern technology, organizations involved in controlling these satellites will need to adopt many of the security practices designed for factories, power companies, and other organizations with ICS.

BOLDLY GOING FORWARD

It is important to remember that satellites are dynamic cyber-physical systems in an unregulated and unpredictable environment.

Collisions,[69] debris,[70] and orbital failures are all realities that can affect entire areas of space in Earth's orbit and any nearby assets.[71] As more satellites fill the sky, the opportunity for and consequences of one or more satellites moving unpredictably—or maliciously—will increase dramatically. Space is likely to become an attractive target to many classes of threat actors, and companies operating in space will need to defend accordingly.



What you can do to mitigate this threat:

- The most important practice is network segmentation—separating OT networks from those that can access the public internet. Complete physical separation or "air gapping" is usually touted as the ideal approach, but strong architectural separation with dedicated security appliances and strict policies at network borders can accomplish similar levels of protection.
- Other practices are more general and include security awareness, network monitoring and inventory, public attack surface reduction, host security and hardening, and vulnerability management. The issue is that many OT-heavy organizations do not understand how relevant or important these IT security practices are to them.

Advanced persistent threats (APTs) using similarly written .Net malware combined with nation states going after rival nation states to use their infrastructure to deploy similar malware will cause attribution nightmares in 2020. A shift to using more advanced Linux malware on infrastructure as more .Net userland malware is deployed will also occur.

- Windows kernel is now heavily defended – making userland malware more prominent.
- Advanced APTs will do more against Linux because of this increased hardening and we expect that to be a major focus for advanced actors in 2020.
- The majority of the recent userland malware found from multiple APTs has been .NET malware.
- Malware written in this intermediary language can be easily modified and an APT could alter a rival APT's malware then deploy it in an operation, causing attribution issues for defenders.
- Many APTs use the same 1-day exploits and lateral movement techniques making attribution more difficult.
- APTs also hacked other APTs in 2019; using rival APT infrastructure to steal victims and deploy their own tools – blurring the lines of attribution.
- APTs could use these blurred lines of attribution to conduct "false flag operations".

WHEN ADVANCED PERSISTENT THREATS ALL LOOK ALIKE

We predict in 2020 that attribution of attacks will become extremely difficult as most, if not all, advanced persistent threats (APTs) continue to rely more heavily on userland malware and userspace tactics, techniques and procedures (TTPs) to conduct operations. This ever-increasing reliance on userland malware and "living off the land" TTPs will continue because Microsoft has hardened the kernel to attacks. Malware written in the .NET intermediate language that relies on simple scheduled tasks to persist has become the favored option for most APTs. This malware presents unique challenges moving forward for cyber threat intelligence, particularly with attribution, because of the nature of the languages and how they can be decompiled and recompiled with multiple nation-state adversaries using others' base implants.

SAME MALWARE, DIFFERENT APT

This new environment where APT tools all look alike and TTPs can be identical is exacerbated by nation-state adversaries that have begun to hack each other's programs and used rival nation-state infrastructure to deploy their own similar tools—further muddying attribution. In additionally, we have seen multiple nation-state programs use the same 1-day exploits within similar timeframes, often deploying similar .NET malware or even using the exact same loading techniques (such as CertUtil and PowerShell). The use of more 1-day exploits by multiple actors all deploying similarly written .NET malware, and even deploying off of a rival's infrastructure, will mean attribution problems in 2020. The smartest APTs will realize the muddying of the attribution waters and will use this to their advantage to hide themselves as a culprit. Even worse, enterprising nation-state groups may seek opportunities for more sinister false-flagging operations and will seek to mimic rival programs and deploy their own variations of rivals' malware.

EXPANDING TARGET ENVIRONMENTS

Finally, malware in this intermediate language also presents unique challenges for detection by defenders and unique opportunities for attackers to move laterally because of the cross-platform ability of malware written in these languages. We also predict a shift by APTs looking for persistence in a network to comprising critical infrastructure nodes running Linux to ensure more sustained access by APTs that are more often settling for living in userland on endpoint machines.

A MOVE TO ACTOR-AGNOSTIC SECURITY

Correct attribution could become nearly impossible and could lead to major geopolitical issues between governments because of false-flagging operations as governments or even as organizations try to determine who attacked them. The ongoing widespread use of .NET-written malware, which is a robust intermediate language, should provide new avenues for hunters, but security operations must be aware that Linux infrastructure is a more valuable target than ever.

In a world where all APTs start to look alike, by happenstance or by design, an actor-agnostic approach to security is due. While it may be hard and against the first natural inclination after an attack to determine the who did this, organizations should try to stop worrying about attribution and take advantage of implementing more userland analytics on endpoints and a focus on hardening Linux infrastructure.

What you can do to mitigate this threat:

- Companies should stop worrying about attribution. Most major companies always want to know "who did this," but the focus really should shift to an actor-agnostic approach.
- The barrier to entry with .Net malware is much lower because it is often easier for seasoned analysts to analyze, leading to greater ability to analyze and pivot.
- Companies should focus more on defending non-Windows infrastructure in 2020 and onward.

An expanding number of threat actors—both state-sponsored and non-state groups—will adopt the tactics demonstrated in previous influence operations to target campaigns in 2020, and a primary objective will be to generate a sense of chaos, undermining public confidence in the election system, infrastructure, and outcome.

Nation state efforts to interfere with the 2016 presidential elections demonstrated an effective playbook for cyber threat actors seeking to disrupt or interfere with election activity.

Proliferation of this model has already been seen in campaigns around the world and will likely be adopted by an even wider array of actors.

Interference in Ukraine's 2019 election may provide a template for the next form of influence operation, a model seeking to cause chaos that could instill distrust and illegitimacy in any election outcome.

DIGITAL ELECTIONS INTERFERENCE

COPYCATS TO COME

Modern IT and social media have provided new vectors to tamper with election outcomes. The manner and scale at which these digital techniques are deployed, especially by malicious actors outside the legal political process, are the primary threat to democracy. Digital election interference rose to the forefront of American public consciousness following the 2016 U.S. Presidential election. Reports that nation state actors sought to influence election results by targeting both voters and U.S. state election infrastructure ultimately resulted in eroded faith and accusations against the integrity of the outcome. Known tactics by the Internet Research Agency—a Russian company with ties to the Kremlin—included the operation of social media "bot" accounts, the usage of political advertisements on social media, and the staging of political rallies to encourage voter abstinence and third-party voting.[72] Additional events by government-affiliated threat actors ranged from vulnerability scans, spear-phishing and denial-of-service attacks, to remote access of voter registration databases. [73], [74], [75]

In 2020, Booz Allen believes this model will be adopted by a wider variety of actors, and the next evolution of election interference will focus primarily on generating a sense of chaos and attempt to undermine public confidence in the election system and infrastructure. Both state and non-state actors will copy and innovate upon previous nation state attack strategies, launching aggressive campaigns seeking to achieve specific political aims or the simple goal of creating discord. Expect multi-pronged strategies using a cohesive marriage of information operations and computer network operations, components that were potentially tested separately in 2016.

GLOBAL INTERFERENCE

In recent years, digital election interference—leveraging a blend of social media influence operations and network exploitation tactics—has become a global phenomenon with malicious campaigns observed throughout Latin America, Asia, and Europe.

Latin America

According to reporting in mid-2016, in Latin America, at least one political consulting firm has reportedly provided services targeting election activities in nine different countries beginning as early as 2005; services ranged from website defacements, to the theft of sensitive data from rival campaign's servers and public distribution of stolen data via tens of thousands of twitter bots.[76] According to reporting in early 2018, due process in Guatemala has also been impacted by digital influence campaigns waged by groups known locally as "net centers" that use hundreds of fake social media accounts to discredit and erode trust in United Nations-backed anti-corruption efforts.[77]

East Asia

Taiwan and Hong Kong have reportedly been subject to influence operation and election attacks from China using collections of bogus online accounts and false media articles. In 2018, following a typhoon that stranded Taiwanese tourists in Japan, fake articles accused the Taipei Economic and Cultural Office in Japan of inaction while alleging that China dispatched buses to help the tourists. Troubled by the claims, the director-general of the office committed suicide before they could be debunked.[78] In addition, during the Taiwan 2018 midterm elections, China successfully ran a "Russian-style influence campaign" that played a potential role in ousting incumbent politicians in favor of pro-Beijing candidates.[79] More recently, in August 2019, Twitter and Facebook announced that they were removing suspected fake accounts allegedly operated by the Chinese government to spread false narratives that negatively portrayed protests in Hong Kong;[80] Twitter also took the additional step of prohibiting state-controlled entities from purchasing ads to promote their content.[81]

Europe

Influence operations have also been observed in Europe. In 2017, an unknown actor attempted to influence the French presidential election by dumping 9-gigabytes of data stolen from now-President Macron's campaign.[82] Though the effects were mitigated by the timing of the release—just prior to a mandatory legal media blackout 2 days before the vote—bots on Twitter enabled the news to trend online and in France.[83]

The proliferation of digital influence operations in recent years demonstrates the accessibility of these tactics to a wide variety of threat actors and the likely further adoption of these activities by new groups for years to come.

Efforts to instill distrust and confusion during election processes could take a number of different forms—from manipulating, encrypting, or wiping voter registration data to create frustration for individuals trying to participate in the election process, to targeting systems used to provide polling information to discourage voter turnout. If voters have doubts about their ability or agency in casting a vote, they may not participate whatsoever.

SOWING ELECTION DISORDER

Looking ahead, the evolution of election-focused influence operations is likely to not only expand in the actors perpetrating it but also change in its overall objective. Rather than favoring one candidate over another, threat actors may seek to degrade the overall legitimacy of the process, regardless of outcome. A model for this may have already been observed in Ukraine. In the lead up to the Ukrainian presidential election in March 2019, campaign staff and security officials reported a wave of malicious activity, including disruptions of campaign websites, spear phishing of government employees, reconnaissance on telecommunications networks supporting presidential election activity—including gathering information on recovery times following disruptions—and undisclosed attacks against critical infrastructure, leading the former head of the Security Service of Ukraine to assert that "the main goal is to destabilize Ukraine, to discredit, to make chaos." [84] [85] By combining social media campaigns and other attacks targeting a wide range of election-related infrastructure, threat actors may seek to generate distrust in the election process overall, effectively hobbling whichever candidate comes out ahead, before they even step foot in office.

What you can do to mitigate this threat:

- Orginizations need to ensure incident response and recovery plans include communications strategies to inform all relevant stakeholders on the scope of any incidents and address false narratives on cyber attacks before they spread.
- Campaign officials may conduct assessments to determine which assets may represent the most valuable targets for threat actors seeking to steal sensitive campaign data to be dumped publicly or otherwise abused.

As non-state actors engaged in regional conflict increasingly turn to cyber operations as a means of asymmetric warfare, their operators and infrastructure will likely rise in priority as a target for conventional military strikes.

In 2019, Israel conducted the first publicly acknowledged airstrike against Hamas infrastructure used to conduct a cyber attack.

Several non-state groups involved in regional conflict or terrorism are developing their capabilities to conduct offensive cyber operations.

Targeting non-state groups and contractors conducting cyber operations instead of an adversary's own cyber resources carries less risk of escalating conflict.

Hotspots of violent regional conflict hold the greatest risk of counter-cyber military force.

CYBER OPERATIONS CARRY INCREASING RISK OF CONVENTIONAL MILITARY RESPONSE

COUNTERING CYBER CAPABILITIES WITH CONVENTIONAL MILITARY FORCE

In May 2019, following a week of violent exchanges of rocket fire from Hamas and airstrikes from the Israel Defense Force (IDF), Hamas cyber operatives allegedly attempted a cyber operation against unspecified Israeli civilian infrastructure.[86] The IDF reportedly repelled the operation, and in response, conducted an airstrike against the Gaza building that purportedly held Hamas's cyber command center. Soon after, the IDF announced the strike over Twitter, the first publicly acknowledged use of conventional military force in response to an attempted cyber attack.[87]

Responding to cyber operations with military force within the context of ongoing armed conflict is not necessarily a new phenomenon. The U.S. has long asserted the right to respond to cyber operations with force and even approached that threshold in 2015 with a drone strike against the ISIS online recruiter, propagandist, and hacker Junaid Hussain.[88] However, the IDF's public acknowledgment of an airstrike in direct response to a cyber attack is novel and may be a harbinger for similar operations in the future.

NON-STATE ACTORS WITH CYBER CAPABILITIES ARE LIKELY TARGETS

In 2020 and beyond, Booz Allen believes foreign states may increasingly target their adversaries' cyber operators and infrastructure with military force during times of conflict. Although it is possible states may target each other's infrastructure directly, it is more likely that states will avoid direct and escalatory confrontation absent the existence of ongoing conflict.[89] Two groups that stand the greatest risk of being targeted with military force in response to cyber attacks are armed non-state groups and government contractors.

ARMED NON-STATE GROUPS

The more likely targets for counter-cyber military force are armed non-state or sub-state forces involved in violent proxy conflicts. In geopolitical hotspots in the Middle East and Africa, regional powerhouse militaries compete violently for political, economic, and sectarian influence. Armed non-state actors frequently fight alongside of and against state-sponsored allies and adversaries. Non-state groups with growing cyber capabilities in these regions, such as Hezbollah, Hamas, and al-Qaeda, are most likely to face retaliatory military force as they increasingly turn to cyber as a means of asymmetric warfare.

CYBER CONTRACTORS AS POTENTIAL TARGETS

Outside of Hamas and Hezbollah, there are few other non-state groups that possess expertise substantial enough to attract retributive counter-cyber force. However, contractors—private groups of cyber mercenaries offering cyber tools and expertise for hire—could also become targets. Contractors are at elevated risk of facing military force if they provide services for states or groups involved in ongoing hostilities.

HEZBOLLAH

Cyber operators or infrastructure used by Hezbollah, a growing political force in Lebanon with a military wing long supported by Iran, is potentially at risk for military counter-cyber targeting. Hezbollah's cyber prowess has grown in recent years, and the expansion of its operations place it at greater risk for a military response from its adversaries. In October 2018, Czech authorities took down servers used by Hezbollah to conduct cyber espionage against targets around the world.[90] Hezbollah previously infiltrated Israel's defense sector in 2015.[91]

Hezbollah's close relationship with Iran places it squarely within the sights of several regional Iranian adversaries. Hezbollah's support of the Assad regime in Syria and the Houthi rebels in Yemen has already brought the group into violent conflict with Saudi Arabia, the United Arab Emirates, and Israel.[92] Any infrastructure used for cyber attacks by Hezbollah-aligned groups located in hotspots for regional conflict like Syria or Yemen could be targeted.

BAHAMUT

South Asia is a potential flashpoint for counter-cyber force. India and Pakistan, conflict-prone and underdeveloped from an offensive cyber perspective, would likely turn to contractors to target each other in times of conflict. Bahamut, a likely India-based cyber contractor that has sold its tools and services to several different groups, including governments, is a potential example.[93] Depending on the level of conflict, Bahamut could be targeted in response to cyber operations—particularly disruptive or destructive attacks—it is hired to conduct in times of escalated hostility between India and Pakistan.[94]

What you can do to mitigate this threat:

- Be aware of the collateral and downstream effects of armed conflict. Motivated states may use force against dual-use infrastructure that could cause interruptions or loss of data to public and private entities outside the targeted organization.
- Leverage a threat intelligence strategy to maintain up-to-date situational awareness and strategic context of the political, military, and economic landscapes in which your company operates.

Nation state actors are poised to use their cyber capabilities to disrupt the 2020 Olympic games.

International athletics federations continue to petition the International Olympic Committee (IOC) to reverse course and ban certain nation states again from Olympic competition.

JPN

Japan has not ceded ground to nation state diplomatic entreats to acknowledge sovereignty claims to islands off Japan's northern coast, prompting opposition nation state military posturing.

NATION STATES POISED TO INTERFERE IN 2020 OLYMPICS

SPECTER OF OLYMPIC BAN THREATENS BLACKLASH

In 2016 and 2018, nation state military hackers failed to discredit Olympic organizers' charges of state-sponsored anti-doping with targeted leaks and then retaliated disruptively against the 2018 Pyeongchang Olympics opening ceremony.[95] These were quintessential nation state military cyber operations, which historically are designed to intimidate, shape narratives, and punish specific geo-political opponents. High tensions between particular nation states and other opponents—namely international sports federations and the Japanese government—make the 2020 Summer Olympics in Tokyo a likely target for nation state cyber operations.

The underlying issues leading to the alleged disruption of the 2018 Winter Olympics opening ceremony remain unresolved. Starting around August 2016, nation state military actors conducted digital espionage and disinformation campaigns aimed at discrediting allegations of their involvement in perpetrating massive athletic fraud via institutionalized doping.[96] Nation state military faketivist groups repeatedly leaked stolen medical exemptions for prohibited pharmaceuticals, claiming to show that detractors were hypocrites abusing legal loopholes.[97] In December 2017, the IOC banned certain nation states from the upcoming games, prompting hackers to escalate cyber attacks. Two hours before the opening ceremony, the hackers deployed destructive worming malware impacting South Korean ski resorts, the games' official website, and the games' IT provider.[98]

A ban on certain nation states competing in the 2020 Tokyo games looms. The IOC has faced widespread criticism for lifting its ban despite those nation states failing to meet agreed-upon deadlines for reinstatement conditions.[99] The International Association of Athletics Federations (IAAF) has extended its ban on athletes from those states competing under their flag 11 times,[100] most recently in June amid continued allegations of impropriety.[101] Nation state-funded media has continued to signal displeasure with the IAAF; it expressed its "sympathy" for Olympic runner Caster Semenya's fighting an IAAF ban over her naturally high testosterone, pointing to questions about the IAAF's testing data.[102] Should new scandals or mounting pressure compel the IOC to ban certain nation states from the 2020 games, those states are likely to use its espionage, disinformation, and disruptive capabilities again to discredit and retaliate against perceived responsible parties.

What you can do to mitigate this threat:

- Monitor a cyber adversary state's government and state-funded media for early indicators and warnings of state narratives and policy directions.
- Track escalating activity in suspected state-sponsored campaigns against relevant target sets. In this Olympics example, early operations might be data leaks targeting organizers and small-scale targeted disruptive attacks in Japan.
- Tailor defenses to your organizations' most pertinent potential adversaries. Practice scenarios mimicking these adversaries and develop associated playbooks.

CONCLUSION

The evolution of next-generation digital transformations also generates a multitude of new security vulnerabilities. Cyber resilience is more critical now than ever. Organizations must address cybersecurity across the entire organization: IT, OT, cloud, and mobile; leverage cyber as a business enabler; and allow the organization to advance proprietary technology, secure intellectual property, protect the extended supply chain, and maintain competitive advantages. Proactive security planning that incorporates enterprise IT, cloud, and third parties minimizes the impact of cyber threats and improves resiliency. Similarly, we recommend thinking comprehensively about security where employees, leadership, and third-party vendors are aligned to create a cohesive and effective cybersecurity program. In our work with the most sophisticated government organizations and leading enterprises, Booz Allen has consistently seen that the most effective cyber defense is having an agile leadership team that continuously prioritizes risk based upon relevant threats.

We believe that the organizations that understand their threat landscape will be the most cyber resilient, ready to mitigate and defend against an increasing number of attacks. Moreover, those that prioritize cyber as an enabler of their digital transformation will realize lasting business value well past 2020.

REFERENCES

1. Team, MSRC. "Corporate IoT - a Path to Intrusion." Microsoft Security Response Center, August 5, 2019. https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/.

2. Nelson, Mike, David Close, Marty Puranik, Richi Jennings, Richi Jennings, and Michael Vizard. "MY TAKE: Here's How 'Bulletproof Proxies' Help Criminals Put Compromised IoT Devices to Work." Security Boulevard. Security Boulevard, August 21, 2019. https://securityboulevard.com/2019/08/my-take-heres-how-bulletproof-proxies-help-criminals-put-compromised-iot-devices-to-work/.

3. Goedert, Joseph. "FBI Adds New Guidance as IoT Proxy Incidents Increase." Health Data Management. Health Data Management, June 17, 2019. https://www.healthdatamanagement.com/news/fbi-adds-new-guidance-as-iot-proxy-incidents-increase.

4. Stupp, Catherine. "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case." The Wall Street Journal. Dow Jones & Company, August 30, 2019. https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402.

5. Hope, Bradley, Warren P. Strobel, and Dustin Volz. "High-Level Cyber Intrusions Hit Bahrain Amid Tensions With Iran." The Wall Street Journal. Dow Jones & Company, August 7, 2019. https://www.wsj.com/articles/high-level-cyber-intrusions-hit-bahrain-amid-tensions-with-iran-11565202488.

6. mame82. "mame82/Misc." GitHub. GitHub, July 9, 2019. https://github.com/mame82/misc/blob/master/logitech_vuln_summary.md.

7. Corfield, Gareth. "Ivan to Be Left Alone: Russia Preps to Turn Its Internet into an Intranet If West Opens Cyber-Fire." The Register® - Biting the hand that feeds IT. The Register, February 12, 2019. https://www.theregister.co.uk/2019/02/12/russia_disconnect_internet_intranet/.

8. Doffman, Zak. "Putin Signs 'Russian Internet Law' To Disconnect Russia From The World Wide Web." Forbes. Forbes Magazine, May 1, 2019. https://www.forbes.com/sites/zakdoffman/2019/05/01/putin-signs-russian-internet-law-to-disconnect-the-country-from-the-world-wide-web/#1c27a3aa1bf1.

9. "Russia to Launch 'Independent Internet' for BRICS Nations - Report." RT International, November 28, 2017. https://www.rt.com/russia/411156-russia-to-launch-independent-internet/.

10. Truong, Mai, and Jessica White. "Freedom Of The Net." Freedom House. Freedom House, October 2018. https://freedomhouse.org/sites/default/files/FOTN_2018_Final Booklet_11_1_2018.pdf.

11. "The Global Rise of Internet Sovereignty." Coda Story, March 21, 2019. https://codastory.com/authoritarian-tech/global-rise-internet-sovereignty/.

12. Boudreau, John, and Xuan Nguyen. "Vietnam Says Google and Facebook May Have Year to Meet Cyber Law." Bloomberg.com. Bloomberg, November 2, 2018. https://www.bloomberg.com/news/articles/2018-11-03/vietnam-says-google-and-facebook-may-have-year-to-meet-cyber-law.

13. Hollingsworth, Julia. "Hong Kong's Summer of Dissent: After Five Weeks of Protest, Where to next?" CNN. Cable News Network, July 16, 2019. https://www.cnn.com/2019/07/15/asia/hong-kong-protest-five-weeks-intl-hnk/index.html.

14. Alper, Alexandra. "U.S. Government Staff Told to Treat Huawei as Blacklisted." Reuters. Thomson Reuters, July 3, 2019. https://www.reuters.com/article/us-china-usa-huawei/us-government-staff-told-to-treat-huawei-as-blacklisted-idUSKCN1TY07N.

15. Martin, Alexander. "No Technological Grounds for Complete Huawei Ban, Say MPs." Sky News. Sky, July 15, 2019. https://news.sky.com/story/no-technological-grounds-for-huawei-ban-say-mps-11763440.

16. "Google's Project Dragonfly 'Terminated' in China." BBC News. BBC, July 17, 2019. https://www.bbc.com/news/technology-49015516.

17. "Mobile Operating System Market Share Worldwide." StatCounter Global Stats. Accessed October 29, 2019. http://gs.statcounter.com/os-market-share/mobile/worldwide.

18. "Mobile Operating System Market Share Asia." StatCounter Global Stats. Accessed October 29, 2019. http://gs.statcounter.com/os-market-share/mobile/asia.

19. "Desktop Operating System Market Share Asia." StatCounter Global Stats. Accessed October 29, 2019. http://gs.statcounter.com/os-market-share/desktop/asia.

20. Cuthbertson, Anthony. "Huawei Says Its Android Alternative Is 60 per Cent Faster." The Independent. Independent Digital News and Media, July 9, 2019. https://www.independent.co.uk/life-style/gadgets-and-tech/news/huawei-android-us-trade-ban-google-china-hongmeng-os-a8996481.html.

21. Bedford, Tom. "Trump Suggests Huawei's Android Ban Could Be over Soon." TechRadar. TechRadar, July 1, 2019. https://www.techradar.com/news/trump-suggests-huaweis-android-ban-could-be-over-soon.

22. Kolodny, Lora. "Former Google CEO Predicts the Internet Will Split in Two - and One Part Will Be Led by China." CNBC. CNBC, September 21, 2018. https://www.cnbc.com/2018/09/20/eric-schmidt-ex-google-ceo-predicts-internet-split-china.html.

23. Beyer, Dirk, and Julie Ward. “Network Server Supply Chain at HP: A Case Study.” Hewlett Packard, June 29, 2000. https://www.hpl.hp.com/techreports/2000/HPL-2000-84.pdf.

24. Robertson, Jordan, and Michael Riley. “The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies.” Bloomberg.com. Bloomberg, October 4, 2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

25. Mott, Nathaniel. “Supermicro: Third-Party Investigation Disproves Bloomberg’s ‘Big Hack’ Claims.” Tom’s Hardware. Tom’s Hardware, December 11, 2018. https://www.tomshardware.com/news/supermicro-denies-bloomberg-big-hack-report,38231.html.

26. Johnston, Phillip. “January 2018: Component Counterfeiting.” Embedded Artistry. Embedded Artistry, January 1, 2018. https://embeddedartistry.com/newsletter-archive/2017/12/4/december-2017-the-future-of-microprocessors-6an72.

27. Admin. “Why So Many Counterfeit Electronic Components in the Market?” Electronic Components News, May 17, 2018. http://www.ecmsnews.com/2018/05/09/many-counterfeits-electronic-components-market/.

28. Wagner, Paul. “Combating Counterfeit Components in the DoD Supply Chain.” DSIAC, April 2015. https://www.dsiac.org/resources/journals/dsiac/spring-2015-volume-2-number-2/combating-counterfeit-components-dod-supply.

29. Morra, James. “Owner of Independent Distributor Charged for Counterfeit Chips Scheme.” SourceToday, May 11, 2018. https://www.sourcetoday.com/distributor-news/owner-independent-distributor-charged-counterfeit-chips-scheme.

30. Cimpanu, Catalin. “Secret Chips Can Be Hidden in Replacement Parts to Spy and Take Over Smartphones.” BleepingComputer. BleepingComputer.com, August 18, 2017. https://www.bleepingcomputer.com/news/security/secret-chips-can-be-hidden-in-replacement-parts-to-spy-and-take-over-smartphones/.

31. Schlafly, Phyllis. “Buying Counterfeit Chips from China.” Phyllis Schlafly Eagles, October 5, 2011. https://www.phyllisschlafly.com/national-sovereignty/buying-counterfeit-chips-from-china-428/.

32. Markoff, John. “F.B.I. Says the Military Had Bogus Computer Gear.” The New York Times. The New York Times, May 9, 2008. https://www.nytimes.com/2008/05/09/technology/09cisco.html?_r=2&partner=rssnyt&emc=rss.

33. “How to Check Original HP Laptop.” community.hp.com, February 19, 2019. https://h30434.www3.hp.com/t5/Notebook-Operating-System-and-Recovery/How-to-Check-original-HP-laptop/td-p/6168735.

34. Tehranipoor, Mark. “Invasion of the Hardware Snatchers: Cloned Electronics Pollute the Market.” IEEE Spectrum: Technology, Engineering, and Science News, April 24, 2017. https://spectrum.ieee.org/computing/hardware/invasion-of-the-hardware-snatchers-cloned-electronics-pollute-the-market.

35. Dunn, Jeff. “99% Of Fake Apple Chargers Fail a Basic Safety Test, New Study Says.” Business Insider. Business Insider, December 2, 2016. https://www.businessinsider.com/apple-fake-chargers-study-2016-12?r=US&IR=T.

36. “Farewell to Counterfeit Electronic Components.” PCBCart. Accessed October 29, 2019. https://www.pcbcart.com/article/content/farewell-to-counterfeit-components.html.

37. Hegde, Arun. “Active Electronic Components Market Size Is Expected to Exhibit US$ 519 Billion by 2026.” Reuters. Thomson Reuters, July 7, 2019. https://www.reuters.com/brandfeatures/venture-capital/article?id=117862.

38. “Farewell to Counterfeit Electronic Components.” PCBCart. Accessed October 29, 2019. https://www.pcbcart.com/article/content/farewell-to-counterfeit-components.html.

39. Wagner, Paul. “Combating Counterfeit Components in the DoD Supply Chain.” DSIAC, April 2015. https://www.dsiac.org/resources/journals/dsiac/spring-2015-volume-2-number-2/combating-counterfeit-components-dod-supply.

40. Winter, Kathy. “For Self-Driving Cars, There’s Big Meaning Behind One Big Number: 4 Terabytes.” Intel Newsroom, April 14, 2017. https://newsroom.intel.com/editorials/self-driving-cars-big-meaning-behind-one-number-4-terabytes.

41. Petit, Jonathon, and Frank Kargl. “Connected Vehicles: Surveillance Threat and Mitigation.” Accessed October 29, 2019. https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp2.pdf.

42. Center, Security. “Auto Tracking Company Leaks Hundreds of Thousands of Records Online.” Auto Tracking Company Leaks Hundreds of Thousands of Records Online, September 21, 2017. https://mackeepersecurity.com/post/auto-tracking-company-leaks-hundreds-of-thousands-of-records-online.

43. “Damn, Missed My Pay Day. (People Are Selling e-Car Credentials?!) Https://T.co/nEpoq37Lzm.” Twitter. Twitter, July 10, 2019. https://twitter.com/GossiTheDog/status/1148979145705218048.

44. “Mbrace.” mbrace | Mercedes-Benz USA. Accessed October 29, 2019. https://www.mbusa.com/mercedes/mbrace.

45. Brustien, Joshua. “Mercedes Thieves Showed Just How Vulnerable Car-Sharing Can Be.” Bloomberg.com. Bloomberg, July 11, 2019. https://www.bloomberg.com/news/articles/2019-07-11/mercedes-thieves-showed-just-how-vulnerable-car-sharing-can-be.

46. "JAGUAR AND SHELL LAUNCH WORLD'S FIRST IN-CAR PAYMENT SYSTEM: Jaguar Media Newsroom." Jaguar Homepage USA, February 14, 2017. https://media.jaguar.com/en-us/news/2017/02/jaguar-and-shell-launch-worlds-first-car-payment-system.

47. Odisseus. "This Is the FIRST TIME Ever in the History of Computer Engineering That There Is a Malware for ARC CPU, & It Is #MIRAI OKIRU!! Pls Be Noted of This Fact, & Be Ready for the Bigger Impact on Infection Mirai (Specially #Okiru) to Devices Hasn't Been Infected Yet.#MalwareMustDie Pic.twitter.com/y8CRwwkenA." Twitter. Twitter, January 14, 2018. https://twitter.com/_odisseus/status/952641540094033920.

48. "Mirai Okiru Botnet Targets for First Time Ever in the History ARC-Based IoT Devices." Security Affairs, January 15, 2018. http://securityaffairs.co/wordpress/67742/malware/mirai-okiru-botnet.html.

49. http://portal.threatbase.csn.internal/#/report/view?id=5a5e7befb932a4c9648aa846

50. Davies, Alex. "The World's First Self-Driving Semi-Truck Hits the Road." Wired. Conde Nast, June 3, 2017. https://www.wired.com/2015/05/worlds-first-self-driving-semi-truck-hits-road/.

51. "AMENDMENTS TO THE GUIDELINES FOR THE ONBOARD OPERATIONAL USE OF SHIPBORNE AUTOMATIC IDENTIFICATION SYSTEMS (AIS) (RESOLUTION A.917(22)) ." INTERNATIONAL MARITIME ORGANIZATION. INTERNATIONAL MARITIME ORGANIZATION, February 26, 2004. https://www.westpandi.com/globalassets/news/110511-imo-resolution-a.95623.pdf.

52. Shepardson, David. "U.S. Commercial Drone Use to Expand Tenfold by 2021: Government Agency." Reuters. Thomson Reuters, March 22, 2017. https://www.reuters.com/article/us-usa-drones/u-s-commercial-drone-use-to-expand-tenfold-by-2021-government-agency-idUSKBN16S2NM.

53. staff, Science X. "Desktop Scanners Can Be Hijacked to Perpetrate Cyberattacks." Phys.org. Phys.org, March 28, 2017. https://phys.org/news/2017-03-desktop-scanners-hijacked-perpetrate-cyberattacks.html.

54. Brown, Francis. "Highway to the Danger Drone." Highway to the Danger Drone. Bishop Fox, August 3, 2016. bishopfox.com/files/slides/2016/Black_Hat_USA_2016-Danger_Drone-Brown_Petro_Latimer-03Aug2016.pdf.

55. Cheseaux, Jonathan. "Wireless Access Point Spoofing and Mobile Devices Geolocation Using Swarms of Flying Robots." Ecole Polytechnique, April 2004. https://smavnet.epfl.ch/pdfs/CheseauxJonathan_SemesterProject.pdf.

56. Ronen, Eyal, and Colin Flynn. "IoT Goes Nuclear: Creating a ZigBee Chain Reaction." Weizmann Institute of Science, 2016. https://eprint.iacr.org/2016/1047.pdf.

57. Davis, Gary, and Toni Birdsong. "What Is Wardriving?" McAfee Blogs, October 28, 2016. https://securingtomorrow.mcafee.com/consumer/identity-protection/wardriving/.

58. "NOTICE ADVISORY TO GALILEO USERS (NAGU) 2019027." NOTICE ADVISORY TO GALILEO USERS (NAGU) 2019027 | European GNSS Service Centre. Accessed October 29, 2019. https://www.gsc-europa.eu/notice-advisory-to-galileo-users-nagu-2019027.

59. Newman, Lily Hay. "Europe's Galileo Satellite Outage Serves as a Warning." Wired. Conde Nast, July 19, 2019. https://www.wired.com/story/galileo-satellite-outage-gps/.

60. "Tracking and Data Relay Satellite System." Wikipedia. Wikimedia Foundation, October 5, 2019. https://en.wikipedia.org/wiki/Tracking_and_Data_Relay_Satellite_System.

61. Will. "GPS Clock Synchronization." Orolia, April 27, 2016. https://www.orolia.com/resources/knowledge-center/gps-clock-synchronization.

62. Estevez, Daniel. "Galileo Constellation Outage." Daniel Estvez, July 16, 2019. https://destevez.net/2019/07/galileo-constellation-outage/.

63. "NASA." Shodan. Accessed October 29, 2019. https://www.shodan.io/report/X8z4Is8F.

64. "2015 ANNUAL REPORT TO CONGRESS." U.S.-CHINA ECONOMIC and SECURITY REVIEW COMMISSION. U.S.-CHINA ECONOMIC and SECURITY REVIEW COMMISSION, November 17, 2015. https://www.uscc.gov/Annual_Reports/2015-annual-report-congress.

65. "TV5 Monde, Russia and the CyberCaliphate." Simply Security News, Views and Opinions from Trend Micro, Inc, June 10, 2015. https://blog.trendmicro.com/tv5-monde-russia-and-the-cybercaliphate/.

66. Mosher, Dave. "Elon Musk Just Revealed New Details about Starlink, a Plan to Surround Earth with 12,000 High-Speed Internet Satellites. Here's How It Might Work." Business Insider. Business Insider, May 16, 2019. https://www.businessinsider.com/spacex-starlink-satellite-internet-how-it-works-2019-5.

67. Suiche, Matt. "Lessons from TV5Monde 2015 Hack." Medium. Comae Technologies, June 15, 2017. https://blog.comae.io/lessons-from-tv5monde-2015-hack-c4d62f07849d.

68. Corera, Gordon. "How France's TV5 Was Almost Destroyed by 'Russian Hackers'." BBC News. BBC, October 10, 2016. https://www.bbc.com/news/technology-37590375.

69. Eddy, Max. “Satellite Communications Hacks Are Real, and They’re Terrifying.” PCMAG, August 9, 2018. https://www.pcmag.com/news/363004/satellite-communications-hacks-are-real-and-theyre-terrify.

70. Ibid, reference 69

71. “Russian and US Satellites Collide.” BBC News. BBC, February 12, 2009. http://news.bbc.co.uk/2/hi/science/nature/7885051.stm.

72. Zissis, Carin. “China’s Anti-Satellite Test.” Council on Foreign Relations. Council on Foreign Relations, February 22, 2007. https://www.cfr.org/backgrounder/chinas-anti-satellite-test.

73. Grush, Loren. “As Satellite Constellations Grow Larger, NASA Is Worried about Orbital Debris.” The Verge. The Verge, September 28, 2018. https://www.theverge.com/2018/9/28/17906158/nasa-spacex-oneweb-satellite-large-constellations-orbital-debris.

74. “U.S. v. INTERNET RESEARCH AGENCY LLC.” IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA , February 16, 2018. https://www.justice.gov/file/1035477/download.

75. “Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations.” U.S. Government, May 8, 2018. https://www.intelligence.senate.gov/sites/default/files/publications/RussRptInstlmt1.pdf.

76. “REPORT OF THE SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION VOLUME 1: RUSSIAN EFFORTS AGAINST ELECTION INFRASTRUCTURE WITH ADDITIONAL VIEWS.” 116TH CONGRESS. Accessed October 29, 2019. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

77. “Background to ‘Assessing Russian Activities and Intentions in Recent US Elections’: The Analytic Process and Cyber Incident Attribution.” U.S. Government/DNI. Accessed October 29, 2019. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

78. Robertson, Jordan, and Michael Riley. “How to Hack an Election.” Bloomberg.com. Bloomberg, March 31, 2016. https://www.bloomberg.com/features/2016-how-to-hack-an-election/.

79. Currier, Cora, and Danielle Mackey. “How an Army of Trolls Protects Guatemala’s Corrupt Elite.” The Intercept, April 7, 2018. https://theintercept.com/2018/04/07/guatemala-anti-corruption-trolls-smear-campaign/.

80. Jakhar, Pratik. “BBC Monitoring – Essential Media Insight.” BBC News. BBC, November 21, 2018. https://monitoring.bbc.co.uk/product/c200fqlq.

81. Rogin, Josh. “China’s Interference in the 2018 Elections Succeeded - in Taiwan.” The Washington Post. WP Company, December 18, 2018. https://www.washingtonpost.com/opinions/2018/12/18/chinas-interference-elections-succeeded-taiwan/?noredirect=on.

82. Keck, Catie. “Facebook and Twitter: It Sure Looks Like China’s Spreading Bullshit About Hong Kong Protesters.” Gizmodo. Gizmodo, August 19, 2019. https://gizmodo.com/facebook-and-twitter-it-sure-looks-like-chinas-spreadi-1837383015.

83. “Updating Our Advertising Policies on State Media.” Twitter. Twitter. Accessed October 29, 2019. https://blog.twitter.com/en_us/topics/company/2019/advertising_policies_on_state_media.html.

84. Auchard, Eric. “French Candidate Macron Claims Massive Hack as Emails Leaked.” Reuters. Thomson Reuters, May 6, 2017. https://www.reuters.com/article/us-france-election-macron-leaks/macron-campaign-emails-appear-to-be-leaked-online-idUSKBN1812AZ.

85. “Hashtag Campaign: #MacronLeaks.” Medium. DFRLab, May 8, 2017. https://medium.com/dfrlab/hashtag-campaign-macronleaks-4a3fb870c4e8.

86. “The Security Service of Ukraine.”. - The Security Service of Ukraine. Accessed October 29, 2019. https://www.facebook.com/SecurSerUkraine/photos/a.1539443172952349/2336143146615677/?type=3&theater.

87. Gilbert, David. “Inside the Massive Cyber War between Russia and Ukraine.” Vice, March 29, 2019. https://news.vice.com/en_us/article/bjqe8m/inside-the-massive-cyber-war-between-russia-and-ukraine.

88. Forces, Israel Defense. “CLEARED FOR RELEASE: We Thwarted an Attempted Hamas Cyber Offensive against Israeli Targets. Following Our Successful Cyber Defensive Operation, We Targeted a Building Where the Hamas Cyber Operatives Work. HamasCyberHQ.exe Has Been Removed. Pic.twitter.com/AhgKjiOqS7.” Twitter. Twitter, May 5, 2019. https://twitter.com/IDF/status/1125066395010699264.

89. “Crossing a Cyber Rubicon? Overreactions to the IDF’s Strike on the Hamas Cyber Facility.” Lawfare, May 9, 2019. https://www.lawfareblog.com/crossing-cyber-rubicon-overreactions-idfs-strike-hamas-cyber-facility.

90. Lawson, Sean. “With Drone Strike On ISIS Hacker U.S. Escalates Its Response To Cyber Attacks.” Forbes. Forbes Magazine, September 12, 2015. https://www.forbes.com/sites/seanlawson/2015/09/12/with-drone-strike-on-isis-hacker-u-s-escalates-its-response-to-cyber-attacks.

91. Waxman, and Matthew C. “Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4).” SSRN, September 11, 2010. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1674565.

92. Cimpanu, Catalin. “Czech Intelligence Service Shuts down Hezbollah Hacking Operation.” ZDNet. ZDNet, October 16, 2018. https://www.zdnet.com/article/czech-intelligence-service-shuts-down-hezbollah-hacking-operation/.

93. “Cyberattack Tied to Hezbollah Ups the Ante for Israel’s Digital Defenses.” The Christian Science Monitor. The Christian Science Monitor, June 1, 2015. https://www.csmonitor.com/World/Passcode/2015/0601/Cyberattack-tied-to-Hezbollah-ups-the-ante-for-Israel-s-digital-defenses.

94. “Saudi-Led Coalition Says Hezbollah Fighters Killed in Yemen Battles.” Reuters. Thomson Reuters, June 25, 2018. https://www.reuters.com/article/us-yemen-security-group/saudi-led-coalition-says-hezbollah-fighters-killed-in-yemen-battles-idUSKBN1JL0YR.

95. Singh, Pukhraj. “Why I Should Not Be Talking about an Indian Cyber Mercenary.” Writings of Pukhraj Singh, May 6, 2019. https://pukhraj.me/2018/12/05/why-i-should-not-be-talking-about-an-indian-cyber-mercenary/.

96. “The Urpage Connection to Bahamut, Confucius and Patchwork.” TrendLabs Security Intelligence Blog, September 12, 2018. https://blog.trendmicro.com/trendlabs-security-intelligence/the-urpage-connection-to-bahamut-confucius-and-patchwork/30.

97. Ellen Nakashima, “Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say,” Washington Post, February 24, 2018, accessed August 2, 2019, https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html?utm_term=.1026c50a5e53.

98. “United States of America vs. Aleksei Sergeyevich et al.” United States District Court: Western District of Pennsylvania, October 3, 2018, accessed October 5, 2019, https://www.justice.gov/opa/page/file/1098481/download.

99. Rebecca R. Ruiz, “U.S. Athletes Reassured After New Russian Hack,” The New York Times, October 14, 2016, accessed October 31, 2016, http://www.nytimes.com/2016/10/15/sports/us-officials-reassure-athletes-after-new-russian-hack-of-medical-files.html.

100. Ellen Nakashima, “Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say,” Washington Post, February 23, 2018, accessed August 5, 2019, https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html?utm_term=.1026c50a5e53.

101. “Russia’s ban for doping upheld months before World Championships in Doha,” BBC, June 9, 2019, accessed August 5, 2019, https://www.bbc.com/sport/athletics/48570272.

102. Ibid, reference 101.

103. “Russia Faces 2020 Olympics Ban Over Alleged Forged Docs – The Times,” The Moscow Times, June 3, 2019, accessed August 5, 2019, https://www.themoscowtimes.com/2019/06/03/russia-faces-2020-olympics-ban-over-alleged-forged-docs-the-times-a65856.

104. Liam Tyler, “Caster Semenya testosterone ruling: Common sense prevails, but we must have sympathy,” RT, <au 2, 2019, accessed August 5, 2019, https://www.rt.com/sport/458202-caster-semenya-testosterone-ruling.

ACKNOWLEDGEMENTS

The 2020 Cyber Threat Trends Outlook contributors

Wade Alt

Michael Sechrist

Jacob Styczynski

Justin Page

Nathaniel Beach-Westmoreland

Omar Ellis

Juliann Tuleya

Brendan Delaney

Sebrena Sawtell

Maria Gupta

About Booz Allen

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that—together—we will find the answers and change the world. To learn more, visit BoozAllen.com.

To learn more, visit BoozAllen.com/MTS

Anil Markose
Senior Vice President
markose_anil@bah.com
+1-917-305-8007

Wade Alt
Vice President
alt_wade@bah.com
+1-571-437-7712

Copyright © 2019, Booz Allen Hamilton, Inc. All rights reserved. Any prediction, conclusion, or recommendation contained in this report should not be viewed as any guarantee or opinion of any future events or future outcomes. Booz Allen Hamilton undertakes no obligation to update any prediction, conclusions, or recommendations to reflect anticipated or unanticipated events or circumstances in this report. Further, we do not guarantee that this document has identified all cyberthreats, or that a security incident or security breach will not occur. Booz Allen Hamilton takes no responsibility and is not liable for reliance by anyone on the information contained in this report, and any reliance is at the sole risk and discretion of the recipient of this report.