RAND CORPORATION

Perspective

Expert insights on a timely policy issue

SIGINT for Anyone

The Growing Availability of Signals Intelligence in the Public Domain

Cortney Weinbaum, Steven Berner, and Bruce McClintock

SIGINT, or signals intelligence, is intelligence gathered from communications, electronics, or foreign instrumentation[1] and has traditionally been considered an inherently governmental function. Historically, only government had the financial means *and* the legal authority to conduct SIGINT activities, and, in our experience, many members of the U.S. government still hold this opinion today. We tested this viewpoint by conducting a market scan to seek examples of how new technologies, innovations, and behaviors are challenging the existing government-only paradigm. We examined the breadth of technologies available now and reported to be released in the near future to understand the capabilities each provides, which audience or market each serves, and what implications each may have for government policy and practices.

This was an exploratory effort, rather than a comprehensive research endeavor. We relied on unclassified and publicly available materials to find examples of capabilities that challenge the government-only paradigm. We identified ways these capabilities and trends may impact the U.S. government in terms of emerging threats, policy implications, technology repercussions, human capital considerations, and financial effects. Finally, we identified areas for future study for U.S. and allied government leaders to respond to these changes.

During our market scan, we found examples of SIGINT capabilities outside of government that are available to anyone. The capabilities we found have applications in maritime domain awareness; radio frequency (RF) spectrum mapping; eavesdropping, jamming, and hijacking of satellite communications; and cyber surveillance. Most of these capabilities are commercially available, many are free, and some are illegal. In our view, the existence of both legal and illegal markets and capabilities results in an environment where SIGINT has been democratized, or available to anyone.

The capabilities we found have implications for the U.S. government and allies. They increase the threat environment by

providing adversaries with capabilities that would otherwise be unavailable, and they have the potential to challenge current U.S. government collection and analysis practices.

The U.S. government has an opportunity to respond to this environment by developing a legal, policy, and regulatory framework for commercial SIGINT; considering changes to its investment strategy; and developing a workforce that makes appropriate use of these capabilities.

In our perspective, the commercialization of geospatial intelligence (GEOINT) provides an illustrative case study of how a historically governmental capability can evolve into a largely commercial enterprise. The commercialization of GEOINT has transformed how governments collect and analyze satellite imagery.[2] It has impacted the quantity and types of overhead imagery capabilities the U.S. government builds and operates.[3] This has led to cost savings when exquisite government-only systems can be used more efficiently by having less-capable commercial systems perform functions that do not require the full capability of government systems. While more limited in scope, developments in non–government-owned SIGINT may enable similar changes.

Democratization or Commercialization?

We began this effort intending to study the commercialization of SIGINT, but we quickly found that *commercialization* was not a suitable term to describe the changes we were finding in the technology sector. By limiting our research to capabilities with a commercial market, we would omit capabilities that remain illegal in the United States yet are readily available to anyone willing to pay for them. While the commercial SIGINT market is worth studying—and we do—it is insufficient to describe the totality of changes in SIGINT-related technologies that are now available to anyone who wants and is willing to pay for them. Throughout this report, we discuss whether each capability is legal or illegal, and how that distinction affects the U.S. government.

The term *democratization* describes when something is accessible to anyone who wants it. We found that democratization is more suitable to the SIGINT environment, and Figure 1 shows the distinction between government-only capabilities, commercialization, and democratization.

Across the technologies investigated, we discovered that nongovernmental capabilities in outer space are—so far—always commercial. Meanwhile, nonspace capabilities, such as cyber and ground-based systems, could be commercial, illicit, or do-it-yourself (DIY). DIY capabilities include devices that could be built with minimal technical expertise using inexpensive components.

Democratized SIGINT Capabilities

We relied on publicly available, open-source information for our research, and this section describes the types of capabilities we discovered. We did not aim to identify all technologies available;

Figure 1. Definitions

Government-only	Capability is built and operated by government(s), or Capability is built and operated by a commercial provider but is only accessible to government(s)
Commercialized	Capability is available for purchase in legal markets
Democratized	Capability is available, either legally or illegally, for purchase or free to anyone who wants it, including as DIY

additional technologies may exist in research and development programs that are not yet public, and some technologies may be available that our research did not find. Some of the capabilities we discovered originate in foreign countries, including capabilities under development in Russia and Israel. In this section, we discuss well-understood and widely adopted commercial capabilities first, followed by emerging capabilities (including those with gray markets or questionable legality), and end with illicit capabilities that exist outside of legal markets.

Some of the technology areas we identified are not new, but we found that they are noticeably more sophisticated than the capabilities previously available to nongovernmental consumers. For example, while RF spectrum mapping is routinely performed to analyze cell phone coverage, and while the basic technology has long been available to hobbyists with small hand-held antennas and spectrum analyzers, it has not been commercially available from satellites that provide global coverage. That situation is about to change.

Within the SIGINT community, practitioners distinguish between signal externals and signal internals. *Signal externals* provide such information as the strength, frequency, and modulation of the signal and can be used to analyze traffic flows, traffic patterns, and network activity. Such information can, for example, be used to improve network management. *Signal internals*, by contrast, reveal the message content being transmitted and may require decryption or language translation. We found that both types of capabilities are available and that different customers require different types of SIGINT.

The technology areas we identified are noticeably more sophisticated than the capabilities previously available to nongovernmental consumers.

Maritime Domain Awareness

Maritime domain awareness is the most mature commercial SIGINT application we found. *Maritime domain awareness* is the effective understanding of any vessels or objects in the maritime domain that could impact security, safety, economy, or the environment.[4] In the early 1990s, the automatic identification system (AIS) was developed as an automatic ship-board tracking system to assist with collision avoidance in densely trafficked coastal areas. Beginning in 2002, the International Maritime Organization mandated AIS use on select vessels, expanding the number of vessels requiring AIS over time. Currently AIS is required on all international ships over 300 tons and on all passenger ships. Originally, AIS transmissions from ships were received by ground stations located along the shore. The advent of commercial, satellite-based AIS detection expanded coverage to the open oceans.

In 2005, a number of government and commercial entities began experimenting with using satellite receivers to detect AIS transmissions. Since 2008, several commercial companies, such as exactEarth, ORBCOMM, and Spire, have deployed constellations of satellites with AIS receivers. These companies provide maritime domain awareness products based on their satellite AIS data, often combined with other sources of data. They also provide satellite AIS data feeds to users and resellers who may combine the AIS data with other sources to generate their own products.

These developments are significant for a number of reasons. Satellite AIS was originally designed to help track compliant vessels in crowded waters but now allows the ability to fuse AIS data with optical and radar imagery and other data sources. Fused data, especially if these data use high-accuracy geolocation tools, could merge information from different sensors and different providers to track compliant ships and "dark" ships—vessels that choose to not broadcast their AIS signal or that broadcast a false (spoofed) AIS signal. When other open-source intelligence (OSINT) is incorporated, further insights can be revealed. Several current or planned commercial imagery satellites include an AIS payload, and at least one low Earth orbit (LEO) satellite communication constellation will host an AIS payload.

Windward, an Israeli company, uses this fused, multi-source analysis. Windward provides maritime intelligence to customers by fusing AIS information with imagery and other current and historical data sources, and applying artificial intelligence algorithms to establish patterns of life and provide alerts about anomalous patterns of behavior.[5] These analyses are used for maritime domain awareness and for more-efficient use of other surveillance platforms and interdiction platforms. Windward also is developing applications for use in financial markets.[6]

RF Spectrum Mapping

We found commercial examples of RF signal monitoring outside of maritime domain awareness. In 2013, Google released its Spectrum Database free to the world, allowing anyone to stake a claim to unused RF spectrum (also called white space). This free offer allows a user to determine whether a spectrum used in a specific geographic region is registered in the database (and therefore allowed by U.S. government regulation)[7] or not registered (possibly indicating a covert use). This capability is useful only within the United States. For farther-reaching RF mapping, space-based capabilities are needed.

An American company, HawkEye360 (or HE360), was formed in 2015 to attempt to launch "the world's first privately-funded constellation of small satellites flown in formation that will be capable of collecting data and generating reports on geolocated wireless signals."[8] HE360 plans to deploy a trial constellation of three satellites for SIGINT applications in late 2017. The HE360 satellites will receive AIS signals, and HE360 also claims that its constellation "will collect information on specific radio signals worldwide to provide high-precision radio frequency mapping and analytics that we can customize to our clients' needs."[9] According to HE360, the signals it plans to collect and analyze are not currently available in the commercial sector. If successful at collection, mapping, and predictive analysis, HE360 would provide an unprecedented intelligence offering to both commercial and foreign government customers.[10]

The proposed commercial RF signal monitoring capability is significant for several reasons. It would allow commercial actors to detect, characterize, and geolocate signals, supporting applications for identifying transportation patterns in congested shipping lanes or by creating maps of areas of spectrum interference.[11] Emitter geolocation also can be used to locate sources of interference, including intentional jammers.

RF spectrum mapping has additional security applications. The Defense Advanced Research Projects Agency, known as DARPA, has a RadioMap program that seeks to provide real-time situational awareness of spectrum use in a local area.[12] DARPA

Satellite eavesdropping was previously the domain of governments and some specialized hobbyists, but we found numerous public examples of tools that are either commercially available or accessible for users to build themselves, with minimal costs and technical expertise.

describes applications of RF mapping that include real-time usage maps for dynamic spectrum access, situational awareness for small tactical units, and support to electronic warfare systems. Satellite-based RF mapping of the type planned by HE360 would expand the coverage from local to global.

Eavesdropping, Jamming, and Hijacking Satellite Systems

Satellites were initially designed without serious consideration of defense mechanisms. Many legacy systems or new commercial systems are vulnerable to a wide variety of signals-related interference, either because the defenses were not available at the time of launch or the costs were determined to be excessive based on the perceived threat. Governments and nonstate actors have exploited the communication structure of satellite systems for years. Our research found that commercial capabilities are rapidly proliferating to exploit satellite signals.

The least-threatening and most-prolific form of signals exploitation is eavesdropping, which also provides the one capability that is clearly SIGINT, rather than electronic warfare. Eavesdropping allows a user to access data transmitted via satellite or other means. Satellite eavesdropping was previously the domain of governments and some specialized hobbyists, but we found numerous public examples of tools that are either commercially available or accessible for users to build themselves, with minimal costs and technical expertise.

One example of satellite eavesdropping was the use of the $26 Russian SkyGrabber program by hackers in Iraq to capture U.S. military Predator drone video feeds in 2009. Insurgents eavesdropped on the unencrypted video feed backhauled from Predator drones through commercial communications satellites.[13] Surprisingly, such encryption weaknesses still exist for some commercial satellite systems. The government addresses this weakness by requiring encryption for military communications that rely on commercial systems, but other nongovernmental traffic through those systems may remain vulnerable.

Eavesdropping is a passive form of signals exploitation, but other, more-active forms of interference also affect commercial providers. Jamming has become the primary cause of the impairment and degradation of satellite services. *Jamming* occurs when the attacker floods or overpowers a signal, transmitter, or receiver, interfering with legitimate transmissions.[14] The jammer's target could be the satellite, a ground station, or a ground satellite dish. Commercial satellites have been victims of intentional jamming for more than three decades. In one of the earliest examples, in 1986, a man used commercially available equipment to intercept, jam, and replace the Home Box Office (HBO) satellite broadcast with his own message.[15]

For most of the past 30 years, commercial providers have avoided modifying their satellites to deal with intentional jamming (as opposed to unintentional interference), citing high costs or simply hoping that jamming incidents would subside. Jamming is actually more frequent now, especially in the Middle East following the Arab Spring and the political unrest in Iran. Two companies, Arabsat and Nilesat, now say that the Arab Spring–related interference has reached a point where it is having a material effect on their revenue. Commercial satellite fleet operator Eutelsat announced in 2013 that it was placing an experimental anti-jamming capability on one of its upcoming satellites to be stationed over the Middle East, a decision prompted by increased intentional interference in the region.[16]

The most concerning form of satellite hacking involves hijacking the telemetry, tracking, and command (TT&C) link in an effort to control the satellite itself. In 2009, security vulnerabilities in satellite communication technologies were discovered that allowed hackers to shut down command-and-control systems and steal data. These vulnerabilities were believed to have been exploited as early as 2007 by Russian hackers who may have been sponsored by the government.[17]

In 2015, a security researcher demonstrated that for $1,000, someone could build a device to send spoofed data to a GlobalStar satellite. GlobalStar's system is used to "monitor industrial critical infrastructure such as pipelines, or to track hikers and other adventurers who use GlobalStar's consumer tracker."[18] The researcher said that, using his device, he can monitor any item being tracked on GlobalStar's network for "several miles" around his location.[19]

The democratization of SIGINT is readily apparent across all satellite system areas—eavesdropping, hacking, and jamming.

Cyber Surveillance

Cyber surveillance has been a topic of extensive study. Several of our RAND colleagues explored what they called "black and gray markets for hacking tools [and] hacking services" in their 2014 report, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*.[20] They wrote:

> [t]he hacker market—once a varied landscape of discrete, ad hoc networks of individuals initially motivated by little more than ego and notoriety—has emerged as a playground of financially driven, highly organized, and sophisticated groups. In certain respects, the black market can be more profitable than the illegal drug trade; the links to end-users are more direct, and because worldwide distribution is accomplished electronically, the requirements are negligible.[21]

Today, hacking tools are marketed for consumers in the open, posing vexing problems for intelligence and law enforcement. Earlier this year, *Bloomberg Businessweek* reported that after Edward Snowden's leaks, "most every country on earth wanted to develop its own mini-NSA."[22] A company called Hacking Team offers annual licenses of $200,000 for its Remote Control System (RCS), a tool that "can invisibly eavesdrop on everything [on a target's computer or phone]." Their clients reportedly have included U.S. government agencies, the Russian intelligence agency FSB, and the

governments of Bahrain, Egypt, Ethiopia, Morocco, Turkey, and Saudi Arabia.[23]

Some hackers have claimed to find weaknesses, called *exploits*, that can take control of any phone without the user's knowledge or the user having to click a link. These exploits, sometimes sold for over one million dollars each, claim to infiltrate the silent SMS-process mobile phones used to load updates and perform administrative tasks in the background without users' knowledge.[24]

Individuals and groups with less money to spend are also welcome in the commercial cyber surveillance market. Documents stolen from two spyware companies, FlexiSpy and Retina-X, show that tens of thousands of customers, "ordinary people—lawyers, teachers, construction workers, parents, jealous lovers—have bought malware to monitor mobile phones or computers" and "may have paid only around $50 to $200 for a monthly or annual spyware subscription."[25] In other words, for minimal cost, anyone can monitor someone else's communications, without a warrant or legitimate authority to do so.

Recent developments show that the technical barriers for conducting broader cyber surveillance, called *bulk collection*, may be lowering. In 2016, Nicholas Weaver, a researcher at the International Computer Science Institute at the University of California-Berkeley, designed and built a small cyber surveillance system for less than $900 in one week. Weaver's system featured capabilities including bulk data collection, search functionality, cookie tracking, anonymous user identification, and the ability to inject malware into targeted computers. According to Weaver, the technologies used to build surveillance systems are "very banal and very basic, it's very well understood technology." He said, "We need to act like every open wireless network or hotel in the Washington [D.C.] area is potentially compromised. And with the low cost of such installation, it doesn't even need to remain the realm of foreign intelligence services."[26]

Capabilities that used to be available only to nation-state peer adversaries are now available to any adversary who wants to use them.

The cyber SIGINT sector offers clients robust capabilities at varying price points or with DIY technologies, and, thus far, vendors and their customers seem undaunted that the use of these solutions against unwitting targets in the United States remains illegal.

Implications for the U.S. Government

The democratization of SIGINT has implications for the U.S. government. We did not find examples of systems that can replace existing government capabilities, but current nongovernmental systems can provide unclassified sources to cue collectors and analysts and facilitate information-sharing with foreign partners. Nongovernmental systems can, for example, be used by the U.S. Departments of Defense and Homeland Security to improve maritime domain awareness. In addition, the capabilities we found could be used—and in some cases, already have been used—against the U.S. government and allies.

The operational environment now includes more actors across the market with access to more-advanced SIGINT capabilities than it did in the past. Capabilities that used to be available only to nation-state peer adversaries are now available to any adversary who wants to use them. This increases risks to government systems, and

it also raises serious concerns about privacy. The government should consider how nongovernmental SIGINT tools could be exploited by adversaries, what the risks are to government operational security (OPSEC) and individual privacy, and what actions the government and allies should take to mitigate these risks.

The U.S. government distinguishes between passive collection capabilities and active transmitters because different agencies and military components have specific authorities for one set of missions or the other. Outside of government, we found these distinctions to be of less concern to users, who instead focus on the result they want to achieve. Therefore, our research includes capabilities the government might consider to be electronic warfare or cyber operations, rather than SIGINT.

We identify several areas where further research and debate is needed to create legal, regulatory, policy, process, and human capital solutions to the challenges of democratized SIGINT capabilities. Such areas yield the following research questions:

- How will prohibitions against the monitoring of U.S. persons be applied when using SIGINT systems and data not controlled by the government?
- What restrictions will apply to the types and quality of information shared with foreign governments, businesses, and nongovernmental organizations?
- How might emerging commercial and democratized capabilities interfere with military, intelligence, and law enforcement operations, and what mitigation approaches should be implemented?
- What criteria should the government use, through the authorities of the U.S. Department of Commerce, to regulate which SIGINT capabilities receive space launch permits and which do not? Should the government similarly regulate nonspace SIGINT capabilities, and if so, how?
- What defensive mechanisms (including policies and procedures) should the Intelligence Community implement to protect intelligence officers from adversaries' use of these capabilities?

The democratization of SIGINT is already in progress, yet these changes have not been widely acknowledged or understood by the U.S. government. The development of commercial GEOINT illustrates that commercial sources can complement government capabilities. Commercial SIGINT could similarly complement government SIGINT, though it will likely do so in different ways. The development of SIGINT capabilities outside of government provides both risks to U.S. security and opportunities for the U.S. agencies that are prepared to act.

Notes

[1]Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, Washington, D.C.: U.S. Department of Defense, November 8, 2010 (as amended through February 15, 2016), p. 217.

[2]Robert Cardillo, Statement for the Record Before the U.S. Senate Select Committee on Intelligence, National Geospatial-Intelligence Agency, September 27, 2016. As of February 24, 2017, https://www.nga.mil/MediaRoom/SpeechesRemarks/Pages/Director-Cardillo-Senate-Select-Committee-on-Intelligence-open-hearing.aspx

[3]National Geospatial-Intelligence Agency, "Joint NGA/NRO Activity to Integrate New Commercial Geospatial Intelligence Capabilities for the Intelligence Community," press release, July 15, 2016. As of February 24, 2017, https://www.nga.mil/MediaRoom/PressReleases/Pages/Joint-NGANRO-activity-to-integrate-new-commercial-geospatial-intelligence-capabilities-for-the-Intelligence-Community.aspx

[4]U.S. Department of Homeland Security, National Plan to Achieve Maritime Domain Awareness, Washington, D.C., October 2005, p. 2. As of October 6, 2017, https://www.dhs.gov/sites/default/files/publications/HSPD_MDAPlan_0.pdf

[5]"The Windward Edge," Windward.eu, undated. As of March 9, 2017, http://www.windward.eu/es/#/solutions/WindwardEdge/; "Windward to Launch Marint Maritime Intelligence Solution," Ship-Technology.com, May 21, 2015. As of March 22, 2017, http://www.ship-technology.com/news/newswindward-to-launch-marint-maritime-intelligence-solution-4582423

[6]Catharine Lawson, "WIRED Money: Windward Brings Real Time Analytics to Maritime Data," July 6, 2015. As of May 10, 2017, http://wired.co.uk/article/wired-money-windward

[7]Kevin Fitchard, "White Spaces Anyone? Google Opens its Spectrum Database to Developers," *Gigaom*, November 14, 2013. As of June 6, 2017, https://gigaom.com/2013/11/14/white-spaces-anyone-google-opens-its-spectrum-database-to-developers/

[8]HawkEye 360, "Allied Minds' Subsidiary HawkEye 360 Raises $11 Million in Series A Financing," web page, November 23, 2016. As of January 30, 2017, http://www.he360.com/allied-minds-subsidiary-hawkeye-360-raises-11-million-series-financing/

[9]HawkEye360, homepage, undated. As of March 22, 2017, http://www.he360.com/

[10]Sandra Jontz, "Industry Bringing Space-Based RF Mapping and Analytics to Commercial Sector," *Signal Magazine*, July 28, 2016.

[11]Jontz, 2016.

[12]Joseph B. Evans, "Advanced RF Mapping (Radio Map)," DARPA, undated. As of May 9, 2017, http://www.darpa.mil/program/advance-rf-mapping

[13]Charles Arthur, "SkyGrabber: The $26 Software Used by Insurgents to Hack into U.S. Drones," *The Guardian*, December 17, 2009. As of February 24, 2017, https://www.theguardian.com/technology/2009/dec/17/skygrabber-software-drones-hacked

[14]Pierluigi Paganini, "Hacking Satellites . . . Look Up to the Sky," InfoSec Institute, web page, September 18, 2013. As of February 24, 2017, http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/#gref

[15]Paul McNamara, "Captain Midnight: 'No Regrets' About Jamming HBO Back in '86," *Network World*, April 26, 2011. As of February 24, 2017, http://www.networkworld.com/article/2229101/security/captain-midnight---no-regrets--about-jamming-hbo-back-in--86.html

[16]Peter B. de Selding, "Eutelsat to Field Test New Anti-Jamming Capability," *Space News*, January 28, 2013. As of March 3, 2017, http://spacenews.com/33333eutelsat-to-field-test-new-anti-jamming-capability/#sthash.6mww3eyv.dpuf

[17]Kim Zetter, "Russian Spy Gang Hijacks Satellite Links to Steal Data," *Wired*, September 9, 2015. As of March 3, 2017, https://www.wired.com/2015/09/turla-russian-espionage-gang-hijacks-satellite-connections-to-steal-data/

[18]Lorenzo Franceschi-Bicchierai, "This $1,000 Device Lets Hackers Hijack Satellite Communications," *Motherboard*, July 31, 2015. As of March 3, 2017, https://motherboard.vice.com/en_us/article/this-1000-device-lets-hackers-hijack-satellite-communications

[19]Franceschi-Bicchierai, 2015.

[20]Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*, Santa Monica, Calif.: RAND Corporation, RR-610-JNI, 2014. As of March 9, 2017, http://www.rand.org/pubs/research_reports/RR610.html

[21]Ablon et al., 2014, p. ix.

[22]Jordan Robertson and Michael Riley, "The Post-Snowden Cyber Arms Hustle," *Bloomberg Businessweek*, January 18, 2017. As of April 17, 2017, https://www.bloomberg.com/news/features/2017-01-18/the-post-snowden-cyber-arms-hustle

[23] Mattathias Schwartz, "Cyberwar for Sale," *The New York Times Magazine*, January 4, 2017. As of April 17, 2017, https://www.nytimes.com/2017/01/04/magazine/cyberwar-for-sale.html

[24] Robertson and Riley, 2017.

[25] Lorenzo Franceschi-Bicchierai and Joseph Cox, "Inside the 'Stalkerware' Surveillance Market, Where Ordinary People Tap Each Other's Phones," *Motherboard*, April 18, 2017. As of April 18, 2017, https://motherboard.vice.com/en_us/article/inside-stalkerware-surveillance-market-flexispy-retina-x

[26] Kim Zetter, "How to Make Your Own NSA Bulk Surveillance System," *Wired*, January 27, 2016. As of March 3, 2017, https://www.wired.com/2016/01/how-to-make-your-own-nsa-bulk-surveillance-system/

About This Perspective

This Perspective examines and challenges the assumption that signals intelligence (SIGINT) is an inherently governmental function by revealing nongovernmental approaches and technologies that allow private citizens to conduct SIGINT activities. We explore four technology areas where nongovernmental SIGINT is flourishing: maritime domain awareness; radio frequency spectrum mapping; eavesdropping, jamming, and hijacking of satellite systems; and cyber surveillance. We then provide areas where further research and debate is needed to create legal, regulatory, policy, process, and human capital solutions to the challenges these new capabilities provide to government.

This research was conducted within the Cyber and Intelligence Policy Center of the RAND National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community. For more information on the Cyber and Intelligence Policy Center, see www.rand.org/nsrd/ndri/centers/intel or contact the director (contact information is provided on the web page).

About the Authors

Cortney Weinbaum is a management scientist at the RAND Corporation. She has spent 14 years in the Intelligence Community and Department of Defense improving policies, practices, and technologies. Previously, she served as an intelligence officer and program manager developing radio frequency and electromagnetic measurement and signature intelligence (MASINT) collection systems.

Steven Berner is a senior engineer at the RAND Corporation. For nine years he led RAND's work for the National Geospatial-Intelligence Agency, including developing a strategy and roadmap for NGA's research and development programs. Mr. Berner has over 40 years of experience in satellite and aerospace programs addressing the overlap of technology, policy, and national security.

Bruce McClintock is an adjunct policy analyst at the RAND Corporation and a retired U.S. Air Force Brigadier General. He served as a special assistant to the commander of Air Force Space Command and as the senior defense official and defense attaché in the U.S. Embassy in Moscow, Russia. He is a command pilot with over 3,500 hours in 35 different aircraft and experience with national security space operations.

Limited Print and Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please visit www.rand.org/pubs/permissions.html.

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. ® is a registered trademark.

For more information on this publication, visit www.rand.org/t/PE273.

© Copyright 2017 RAND Corporation

RAND CORPORATION

www.rand.org

PE-273-OSD