From AFIO's THE INTELLIGENCER
JOURNAL OF U.S. INTELLIGENCE STUDIES
Volume 24 • Number 3 • Winter 2018-19
$15 single copy price

Association of Former Intelligence Officers
7700 Leesburg Pike, Suite 324
Falls Church, Virginia 22043
Web: www.afio.com, E-mail: afio@afio.com

II. Current Issues

Cyber Intelligence

by Robert M. Clark
and
Peter C. Oleson

Introduction

In his March 2018 presentation before Congress on the Worldwide Threat Assessment, Director of National Intelligence (DNI) Daniel Coats listed cyber first among the multiplicity of threats facing the U.S.

The potential for surprise in the cyber realm will increase in the next year and beyond as billions more digital devices are connected – with relatively little built-in security – and both nation states and malign actors become more emboldened and better equipped in the use of increasingly widespread cyber toolkits. The risk is growing that some adversaries will conduct cyberattacks – such as data deletion or localized and temporary disruptions of critical infrastructure – against the United States in a crisis short of war.

Ransomware and malware[1] attacks have spread globally... The availability of criminal and commercial malware is creating opportunities for new actors to launch cyber operations.

[W]e remain concerned by the increasingly damaging effects of cyber operations and the apparent acceptance by adversaries of collateral damage.[2]

The government and corporations are investing significant resources to defend against cyber intrusions. In response to continuing foreign nation-state cyberattacks in November 2018 Congress established a new entity within the Department of Homeland Security (DHS), the Cybersecurity and Infrastructure Security Agency with enhanced powers.

Both defensive cyber security and offensive cyber operations depend on good cyber intelligence for warning and assessment of hostile players' intentions and capabilities. Both of these are traditional intelligence functions. Many experienced observers have raised questions about the country's approach to the cyber environment.[3] At the August 2018 DoDIIS[4] conference Principal Deputy DNI Sue Gordon stated that the Intelligence Community's #3 priority was "[d]eveloping a comprehensive cyber strategy."[5] The House Armed Services Committee asked the DoD for a briefing on standardizing doctrine for cyber, developing all-source cyber intelligence analysts, and resourcing cyber intelligence analysis at the new Cyber Command (CYBERCOM). One observer asked: "Does DoD know how to supply intelligence for cyber ops?"[6] This raises the question: Should cyber become a new Intelligence Discipline (INT)?

Before exploring that question, it's worth summarizing briefly the existing INTs. Some have long histories. But modern technologies in sensing and computation have transformed all INTs in many ways and created new ones. Technical INTs evolved during the First World War and came into their own in World War II. As signals and imagery intelligence (SIGINT and IMINT) required technically competent people, they developed independently within their own unique organizations. These became known as "stovepipes" within the Intelligence Community.

The Traditional INTs

HUMINT Human source intelligence is the oldest form of intelligence, but has evolved significantly in its tradecraft with the development of the other INTs, all of which enable various types of HUMINT operations. HUMINT also contributes to each of the other INTs. For example, HUMINT helps SIGINT by stealing foreign codes; HUMINT operators take ground-based, airborne, and undersea imagery; they also collect published and unpublished materials; implant technical sensors

[1] Ransomware is malicious software (malware) that seizes and encrypts the memory of a targeted computer and demands payment, often in BitCoin, to release the code to unencrypt the hostage memory.

[2] Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community, Daniel R. Coats, Director of National Intelligence, 6 March 2018.

[3] See, for example, Mark Pomerleau, "New Leader Wants Cyber Command to be more Aggressive," CYBERCOM, FifthDomain, July 24, 2018, *https://www.fifthdomain.com/dod/cybercom/2018/07/23/*; Gus Hunt (former CTO at CIA) interview at *http://www.fifthdomain.com/*; "Cyberthreats have changed dramatically in recent years, but our national approach to cyber defense has not." David H. Petraeus and Krian Sridhar, "The Case for a National Cybersecurity Agency," 09/05/2018, *https://www.politico.com/agenda/story/2018/09/05/cybersecurity-agency-homeland-security-000686?cid=apn* ; and James Stavridis, "We're Heading Toward a Cyber Pearl Harbor," In Focus, *Tufts Magazine*. Fall 2018. *https://tuftsmagazine.com/in-focus/cyber-insecurity*.

[4] DoDIIS is the Department of Defense Intelligence Information System.

[5] *https://www.c4isrnet.com/show-reporter/dodiis/2018/08/17/*.

[6] Mark Pomereau, *http://www.fifthdomain.com/*.

for MASINT collection; and collect geospatial information. CIA remains the central node for HUMINT operations and coordinates the HUMINT activities of DIA and the military services.[7]

SIGINT Cryptanalysis, which long predates radiofrequency (RF) COMINT, is viewed as the most sensitive of SIGINT activities. The British developed a system of security compartments severely restricting dissemination of communications intelligence (COMINT) derived from code breaking. The US Army and Navy adopted the British model during World War II.[8] Less restricted was unencrypted RF COMINT, such as high frequency direction finding (HFDF), used against U-boats, and intercepts of Luftwaffe air-to-air and air-to-ground transmissions and German navigational beam transmissions gathered by the Royal Air Force Y-Service. The WW II UKUSA agreement on SIGINT later evolved into the "Five Eyes" international SIGINT community comprising the UK, US, Canada, Australia, and New Zealand. After various reorganizations in 1952 the National Security Agency (NSA) became the SIGINT stovepipe.

IMINT Airborne imagery intelligence began during WW I and grew dramatically during WW II when specialized aircraft were configured to collect photos and large analytical organizations were established to perform imagery analysis of enemy targets. The advent of the Cold War the need for IMINT of the Soviet Union led to the development of the U-2 program by the Central Intelligence Agency (CIA). The U-2 development, begun in 1955, was the first "black program" covered by security compartmentation (codeword TALENT).[9] In 1960 the development of photoreconnaissance satellites was also compartmented, and the product of satellite reconnaissance was covered by the codeword KEYHOLE. The National Reconnaissance Office (NRO) became the stovepipe for collection by both imagery and SIGINT satellites, though processing and exploitation continued to be done by the National Photographic Interpretation Center (NPIC) and NSA, respectively.[10]

The Newer INTs

Since the late 1970s three new independent INTs have been formed. All three have longer histories as intelligence sources but were recognized as separate INTs only since the 1970s.

OSINT Open source collection and analysis is age old. Its defining characteristic is that the information is publicly available for gathering. Traditionally the work of librarians, in WW II the monitoring of foreign radio broadcasts by the Federal Communications Commission (FCC) became an important element. After the war this task was transferred to CIA's Foreign Broadcast Information Service (FBIS). While all agencies in the Intelligence Community engage in open source (OSINT) intelligence to support their primary focus, CIA took the lead in consolidating open source exploitation of print and electronic sources. OSINT was recognized as an independent INT (but interrelated with other INTs) when the DNI established the DNI Open Source Center, which remained housed within the CIA. With the explosion of openly available information as the result of modern communications technology, especially the Internet, OSINT has faced the same challenge as SIGINT and imagery: an overwhelming quantity of collected materials that outstrip the ability to process and analyze.

MASINT Scientific and technical analyses have long supported intelligence. These have enabled the "detection, location, tracking, identification, and description of unique characteristics of fixed and dynamic target sources."[11] In the late 1970s, the House Permanent Select Committee on Intelligence (HPSC(I)) pressured the DoD to consolidate many disparate sensory efforts the HPSC(I) viewed as intelligence-related into a category to allow oversight.[12] These included programs

[7] For some Counterintelligence is a separate discipline. The authors of this paper believe counterintelligence is a purpose or activity to which the various collection disciplines contribute.

[8] Compartments were designated by codewords, for example: ULTRA for decrypted German Enigma transmissions, FISH and TUNNY for decrypted German radio teletype messages, MAGIC for Japanese diplomatic and naval messages.

[9] CIA also developed the A-11 Mach 3 supersonic high altitude reconnaissance aircraft. That program morphed into the SR-71 program run by the Air Force.

[10] For many years the NRO was a hybrid organization consisting of largely independent Air Force, CIA, and US Navy program offices that often competed against each other for both imagery and SIGINT developments.

[11] John L. Morris and Robert M. Clark, "Measurement and Signature Intelligence," in Mark M. Lowenthal and Robert M. Clark, *The 5 Disciplines of Intelligence*, Washington, D.C.: CQ Press, 2016, p 160-1. This chapter explains in detail the history of MASINT, its many uses, many of its sensor systems, and its management.

[12] The newly formed HPSC(I) was competing with the established House Armed Services Committee (HASC) for jurisdiction over all intelligence and related activities, seeking a broader charter than that of its Senate counterpart, the Senate Select Committee on Intelligence

that operated in the electromagnetic, acoustic and seismic spectrums, as well as material sciences, which took on the moniker of Measurement and Signature Intelligence (MASINT). DoD established a management structure called "Tactical Intelligence and Related Activities (TIARA)," which evolved into today's Military Intelligence Program (MIP). MASINT was included and overseen by the Central MASINT Office (CMO), established in 1992 within the Defense Intelligence Agency (DIA), although many of its operations remained within the various military services, CIA and NSA.

The various sub-disciplines of MASINT grew over time to include: electro-optical sensing across the spectrum from ultraviolet to long wave infrared; radar sensing, including bi-static and multi-static, synthetic aperture, and over-the-horizon; laser imaging; radiofrequency collection, including electromagnetic pulse, wideband radar, unintended radiation, directed energy, and lightning; geophysical sensing in the acoustic, seismic, and magnetic realms; nuclear radiation; and materials sampling, including effluents, particulate debris, and biological and chemical warfare related observables.[13] One important characteristic of MASINT is its non-literal aspect, which requires often substantial processing of data and subsequent technical scientific analysis to derive usable intelligence.

GEOINT Geospatial Intelligence (GEOINT) is the marriage of IMINT and geographical information (primarily cartography). It is a hybrid of both to provide a value-added approach.[14] As such it encompasses both collection and analysis of imagery (IMINT).

GEOINT evolved from aerial reconnaissance in WW I and WW II, and especially from the development of satellite imagery collection after 1960. Classified satellite imagery and the development of the Global Positioning System (GPS) revolutionized the preciseness of map making. Even more significant was the development of unclassified remote sensing of the earth by scientific and commercial satellites. LandSat was the first in 1972. Massive volumes of imagery later became available with the proliferation of unmanned aerial vehicles (UAVs) and video mosaics. Together these provided data across a broad spectrum that enabled analyses not possible from earlier panchromatic imagery. Visual (film based and electro-optical) imagery, multi-spectral and synthetic aperture radar imagery, and laser imagery (LIDAR) are subsets of IMINT.

The amalgamation of imagery interpretation and mapmaking in the 1990s enabled the growth of GEOINT. Several organizational developments helped, from the establishment of the National Imagery and Mapping Agency (NIMA) in 1995, which combined the Defense Mapping Agency with the National Photographic Interpretation Center (NPIC) and independent CIA and DIA imagery offices, to the culturally transforming evolution into the National Geospatial-Intelligence Agency (NGA) in 2003.

GEOINT draws from all of the other INTs, integrating their data into geographically related context. Imagery, SIGINT, HUMINT, OSINT and MASINT contribute to GEOINT.[15]

What Constitutes an INT?

The authors are not aware of any publication defining the essential elements of an INT. The term "INT" is generally accepted as referring to an intelligence collection discipline that produces raw intelligence.[16] But all existing INTs also require some type of analysis, even if limited to simply evaluating the source. Following are some of the major characteristics that seem applicable to existing INTs.

Distinguishable From Other INTs

An INT should have features that distinguish it from other INTs. Some overlap is inevitable, but an INT also has to have unique and readily identifiable characteristics. GEOINT, which overlaps with every other INT, nevertheless has a distinguishing feature: the focus on locating and characterizing objects and activities on earth. MASINT, an amalgamation of subdisciplines, is distinguished by its focus on measurements and signatures (physical, chemical, radiological, and electromagnetic).

(SSC(I)).

[13] Morris and Clark, p 177.

[14] "The term 'geospatial intelligence' means the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information." US Code, Title 10, section 467 (10 U.S.C. 467).

[15] For a detailed overview of GEOINT see Darryl Murdock and Robert M. Clark, "Geospatial Intelligence," in Lowenthal and Clark's *The 5 Disciplines of Intelligence*. For the history of NGA see Gary E. Weir, "The Evolution of Geospatial Intelligence and the National Geospatial-Intelligence Agency," in Peter C. Oleson, editor, *AFIO's Guide to the Study of Intelligence*, at *https://www.afio.com/publications/Guide/index.html?page=1*.

[16] Mark M. Lowenthal and Robert M. Clark, *The 5 Disciplines of Intelligence*, Washington, D.C.: CQ Press, 2016., p 1-2.

An Underlying Body of Tradecraft

HUMINT, SIGINT, GEOINT, and OSINT all have a defined tradecraft, typically including subdisciplines that have their individual tradecrafts. HUMINT has distinct tradecrafts for clandestine collection (the classic spy), elicitation, and interrogation. SIGINT has its own subset for cryptanalysis, ELINT and FISINT processing and analysis. MASINT subdisciplines all have unique tradecrafts. These generally require unique technical expertise or specialized processing and analysis, or both. There also exist a set of recognizable professional standards for every INT discipline.

A Defined Management Structure

An INT must have significant importance – enough to demand primary managerial attention. That means that it must require specialized "care and feeding": hiring, training, research, and dedicated funding. It requires a collection management structure that can secure funding and adjudicate competing collection priorities. That implies that some agency is the functional manager for the INT, even though other agencies may produce raw intelligence within it; for example, CIA and DIA both produce HUMINT, though CIA is the functional manager. Several agencies produce MASINT, though DIA is the functional manager.

Unique Nature of the Sources and Tools

An INT is expected to have dedicated collection assets (though it may also depend on collection done by other INTs). It must have a specialized set of tools, processes, and analytic procedures for turning collected material into raw intelligence. Some INTs – GEOINT and OSINT, for example – also must rely on sources from outside the Intelligence Community. Others – HUMINT, SIGINT, and MASINT – rely almost exclusively on their own collection assets.

The challenge in most intelligence collection disciplines for years has been summed up in the three words "volume," "variety," and "velocity;" they have been used in reference to SIGINT, GEOINT, and OSINT. All cite the same problem – sifting through the vast amount of available material to target the material that is of intelligence value (for translation in the case of OSINT and COMINT, or detailed exploitation for GEOINT and ELINT.)

The Nature of Cyber

Cyber operations come in three major forms: computer network defense, computer network attack, and computer network exploitation:

1. **Computer Network Defense (CND).** Describes the actions taken to protect, monitor, analyze, detect, and respond to network infiltrations or unauthorized activity within information systems and computer networks.
2. **Computer network attack (CNA).** CNA operations are conducted with the intent to degrade, disrupt, deny, or deceive the target. The effects of CNA typically are readily observed.
3. **Computer network exploitation (CNE).** The objective here is to target the opponent's Internet or an intranet (a privately maintained computer network that requires access authorization and may or may not be connected to the web via an administrative computer), but not for attack. Instead, the focus is on collection operations where the network continues to function normally.

When we consider CYBERINT, we tend to think about the third type of these three. But they are all closely interrelated, and CYBERINT must support CND by providing intelligence about an opponent's CNA or CNE threat. Any consideration of cyber as a separate INT must deal with that interrelationship, much as SIGINT does. COMINT, for example, deals with cryptanalysis – an intelligence function. But cryptanalysis is in turn closely connected with encryption means and other forms of defense against an opponent's COMINT. Both COMINT and ELINT have to coordinate with military operations; if you conduct electronic or kinetic attack against an emitter, you no longer can gain intelligence from it. The same is true of CNA; once you attack an opponent's network, further CNE becomes difficult at best.

With that introduction, let's consider the primary means and targets of CNE.

Means and Targets of CNE

The CNE target is almost always sensitive information held in a computer somewhere or in transit across a network. The primary means of obtaining access to that information is via the Internet.

Internet

Much of the intelligence information obtained via the Internet is openly available: blog posts, news items, tweets… Being readily obtained and analyzed, this material doesn't fit as CNE; it's basically open source, and treated as such.

Sensitive material that the owner wishes to protect, whether in a computer or in transit, fits into a different category. It can often be acquired, given the tools and methodologies that hackers know well. In that respect, it resembles COMINT and uses similar processes, albeit with a unique set of tools. Collection against smart phones, smart watches, and other devices that connect to the web (comprising the Internet of Things) has its own set of processes and tools, but also resembles COMINT in its basic form.

Much of the material of intelligence interest that is available via the web requires access to protected regions of the web, known as the "Deep Web" and "Dark Web."

The Deep Web refers to the vast part of the Internet that is not indexed and therefore not normally visible or accessible from typical search engines. Access-restricted commercial databases, websites, and services comprise much of the Deep Web. Special browser software such as Tor (originally created by the US Navy to transfer files securely) is required for access. The Tor software makes use of a set of virtual private networks, allowing users to securely travel the Deep Web and remain anonymous. It protects users by bouncing their communications around a distributed network of relays run by volunteers around the world, which prevents others from watching users' Internet connections to learn what sites they visit, prevents the sites that users visit from learning their physical location, and lets users access sites that are blocked to anyone without permission. Government databases, such as those maintained by the National Aeronautics and Space Administration (NASA) and the US Patent and Trademark office, also use the Deep Web space for obvious reasons.

Within the Deep Web lies what is often referred to as the Dark Web. Much of the Dark Web content fits well with the name: It includes all types of black markets, illicit drug traffic, fraud-related material, and illegal pornography, along with scores of scams and hoaxes. But, the Dark Web also is used for political discussion groups, whistleblowing sites, and social media sites often to avoid government censorship. Tracing the source of a post in the Dark Web can be very difficult.

Intranets and Standalone Computers

While internet-based collection is widely practiced, cyber collection predates the popularization of the Internet. Intelligence services were targeting standalone computers and intranets well before that time.

An intranet is an internal network that people can access only from within their organization or trusted group. It is intended as a place to securely share files or sensitive documents. Some intranets are not connected to the Internet; others have Internet access, but only through a gateway administrator from within the organization. Intelligence is typically concerned with the type of intranet that connects to the Internet but has some form of protection. These virtual private networks (VPNs) allow people to operate with an expectation of privacy on the Internet. They are profitable targets for CNE, if you can get past the firewall that protects them from intrusion.

Attacking a network that is physically isolated from the Internet (a private intranet) or a single computer that never connects to the Internet requires a different type of effort from that used in CNE. The collector has to gain physical access to the computer or the intranet in some way – through a USB drive, a network jack or cable, or some similar device. And there must be some means for exfiltrating the information obtained, either by the same physical access or by inserting a radiofrequency transmission device into the system. Gaining direct access to an isolated intranet or a standalone computer on a continuing basis requires special effort. But information technology systems rarely exist for long periods in isolation. Upgrades, patches, software fixes, and new hardware and software have to be added to these systems, and all of these provide opportunities for access.

Technically, standalone computers aren't targets of CNE because by definition, they aren't part of a network. But they are important targets of CYBERINT, nevertheless, as they often are not connected to a network in order to protect the information they contain – as the following example illustrates.

In 2003, the Syrians began to construct a nuclear reactor near the town of Al Kibar. The reactor was a near-duplicate of one at Yongbyon, North Korea, and was built with North Korean assistance. It apparently was intended to produce fuel for nuclear weapons. On March 7, 2007, covert operations specialists from Israel's Mossad broke into the Vienna home of Ibrahim Othman, head of the Syrian Atomic Energy Agency. Once inside, they hacked into Othman's computer and copied about three dozen photographs. These proved to be photographs taken from inside the Al Kibar complex. The photos confirmed that Al Kibar indeed housed a copy of the Yongbyon reactor; they even included photographs of North Korean technicians at the facility.[17]

Field operations such as the Israelis conducted are commonly used to access intranets and standalone computers. This category encompasses deployment of any CNA or CNE tool through physical access or proximity. In intelligence, these are called HUMINT-enabled operations; in the world of hackers, they are usually referred to as social engineering. They encompass such classic HUMINT techniques as gaining access under false pretenses, bribery or recruitment of trusted personnel in a facility, and surreptitious entry. HUMINT-enabled operations are often facilitated by human error or carelessness, and complex intranets are particularly susceptible to both.

Technology has provided another option for cyber collection; it has allowed us to hide malware in many places, and the supply chain (all the way from component manufacturer to end user) is a particularly attractive place. Anyone in the supply chain before sale has the access necessary for inserting malware in a computer or other electronic device. Such embedded malware is difficult to detect, and most purchasers do not have the resources to check for such modifications.

The hardware can be modified in ways that are not readily detectable, but that allow an intelligence service to gain continuing entry into the computer or communications system. Targeted components can be add-ons that are preinstalled by the computer manufacturer before the computer is sold. A user may not even use the vulnerable add-on or be aware that it is installed. Malware inserted in a computer before sale can call home after being activated, exfiltrate sensitive data via USB drives, allow remote control of the computer, and insert Trojan Horses and worms.[18] And, such backdoors are not limited to software installed on the computer. Hardware components such as embedded radio-frequency identification (RFID) chips and flash memory also can be the sources of such malware.

Chinese companies have a history of installing such malware in their electronics – most often in smartphones and laptops. The malware typically includes a backdoor designed to collect sensitive information without a user's knowledge or consent. Shanghai Adups Technology Company has supplied firmware to manufacturers who pre-installed it in mobile phones. The included malware collects data such as users' text message content, contact lists, call histories, location data and, phone identifier numbers. Lenovo has repeatedly used Windows features to preinstall unremovable rootkit software in its computers. The information is mostly used for commercial purposes (target advertising), but the Chinese government has access to material collected through the malware.[19]

Does CYBER Fit the Generally Accepted Characteristics of an INT?

The answer to that question is both yes and no. Consider how it fits the previously described characteristics that define INTs.

Distinguishable from Existing INTs

CYBERINT is not easily separated from the established INTs. It overlaps with HUMINT, OSINT, and SIGINT. Much of the most sensitive cyber material is encrypted, so it overlaps with cryptanalysis. CYBERINT also overlaps with RF MASINT (in collecting emanations, for example).

An Underlying Body of Tradecraft

CYBERINT has its own tradecraft; its practice requires unique technical expertise. Applying the tools and talents used in hacking; conducting forensics of the open, Dark, and Deep Webs; inserting malware into hardware and software – all depend on technical specialties that the five traditional INTs apply only peripherally. CYBERINT has its own specialized processing and analysis methods, though breaking encryption – which cyber collection inevitably must encounter – requires the unique expertise of COMINT analysts. And the hardware expertise needed to install malware into the supply chain is similar to that used in audio/video operations – a HUMINT discipline. Social engineering, of course, is a HUMINT skill.

[17] On September 6, Israeli Air Force planes bombed and destroyed the site. David Makovsky, "The Silent Strike," *New Yorker*, September 17, 2012, *http://www.newyorker.com/magazine/2012/09/17/the-silent-strike*.

[18] A Trojan Horse is a piece of malware that appears innocent but clandestinely enables hidden, and often hostile, functions. A worm is a piece of self-replicating malware that adversely affects the operation of computer software and hardware.

[19] Ryan Neuhard, "Flawed by Design: Electronics with Pre-installed Malware," *Georgetown Security Studies Review*, May 23, 2018, *http://georgetownsecuritystudiesreview.org/2018/05/23/flawed-by-design-electronics-with-pre-installed-malware/*.

A Defined Management Structure

Cyber collection today has dedicated collection assets, but it does not have a central management structure. Management is in fact divided among existing INTs, either based on collection means (Internet access versus HUMINT-enabled or other access methods) or on the collection target (e.g. financial crime, terrorists, military forces, counternarcotics). And as noted in a later section, "Who is in Charge," DoD and DHS have management responsibilities for cyber operations that include CNE. For perspective, though, GEOINT management was divided between imagery and mapping organizations prior to the creation of NIMA. Management of CYBERINT today resembles the dispersed management that MASINT had prior to its establishment as an independent INT.

Unique Nature of the Sources and Tools

The tools of CYBERINT are widely available to governments, industry, and individuals. Exploits are shared freely among hackers via the web. But commercial and private availability is not unique to CYBERINT. COMINT receivers are in wide use, in the form of police and emergency services scanner radios. Imagery is collected by drones operated by companies, individuals, and criminal groups. OSINT and both overt and clandestine HUMINT are routinely practiced by multinational companies (e.g., research, "dumpster diving," and undercover investigations).

Cyber requires participation of the private sector, not just in developing hardware and software, but in collecting intelligence. Because commercial entities are often the target of CNE and CNA, cyber threat intelligence depends heavily on inputs from the private sector. Most government entities (including state level governments) are also CNE and CNA targets. Commercial and governmental entities therefore are sources of threat intelligence to a degree unmatched by other INTs.

CYBERINT faces the same challenge of existing INTs in dealing with what is commonly called "Big Data." Like COMINT, Cyber can be targeted on a single electronic device that is of known intelligence interest, or it can be required to sift through vast quantities of material.

Issues

Anytime there is major change in an INT or the proposal to create a new one, significant issues arise. This is true with cyber as it was with GEOINT and MASINT. What's the definition? What are the boundaries? Who is in charge? What are the resources? What are the legal and policy issues governing operations? And others.

Cyber and CYBERINT Definitions

"Cyber" is a new term popularized by Vice Admiral Mike McConnell when he was the Director of NSA.[20] Its definition, however, is important to a number of the other questions raised above.

The definitions of cyber and Cyber Intelligence vary. Some view cyber only as a domain, akin to ground, sea, air, and space.[21] Some view it as a technology.[22] One senior military officer has labeled cyber as a weapon system.[23] Cyber intelligence is seen by some as a newer subset of SIGINT.[24] Others view it as a separate entity – a new INT. Each is correct depending upon one's point of view and assumptions.

A 2013 industry/government study group noted: "[W]hile there is not a currently accepted definition for cyber intelligence, it should not be limited to an understanding of network operations and activities... [C]yber intelligence is not a collection discipline such as Signals Intelligence (SIGINT) or open Source Intelligence (OSINT);... it is an analytic discipline relying on information collected from traditional intelligence sources.[25]

A student studying the question of definition wrote:

> *"Cyber is presently an ill defined concept in the intelligence community; while attempts have been made to formalize a definition of cyber, its practices, methods, and limitations are so alien to anything else in the history of intelligence that hammering down a single,*

[20] July 24, 2018 email to the authors from Rich Haver.

[21] One responder to the authors' survey of opinions stated: "I think of cyber as the operational domain: air, sea, land, space, cyber. In that framework, cyber cannot be an INT.... Instead, I think it makes sense to conceptualize the collection of information from the cyber domain as a variant of SIGINT...updated to new technologies..." July 19, 2018 email to authors from Steve Marrin, professor at James Madison University.

[22] "[C]yber is a technology, a means, but not an INT. Just like satellites are means. It is also an issue, like WMD. So, there can be intelligence about cyber but that does not make it an INT." July 18, 2018 email to the authors from Mark Lowenthal, former Assistant DCI for Analysis and Production.

[23] "Cyber is a weapon system, not a service." LGEN Stephen G. Fogarty, USA, CO Army Cyber Command. Robert K. Ackerman, "Convergence Guides Army Cyber," *Signal*, August 2018.

[24] "I don't think "Cyber" represents a new 'INT.' To me, it is most closely akin to, and an outgrowth of, traditional cryptology. It has many of the same traits (it's 'out there,' in the electronic ether; it has both offensive and defensive dimensions)." July 23, 2018 email to the authors from James Clapper, former DNI.

[25] INSA Cyber Intelligence Task Force, Operational Levels of Cyber Intelligence, September 2013.

> *unified definition is difficult at best. The main problem with finding a concrete definition is that cyber is so versatile that it fulfills many roles simultaneously. Cyber has become a lynchpin in nearly all other disciplines, many of which have come to rely on cyberspace.”*[26]

One of the authors of this article has previously defined cyber intelligence as

> *“Collection that is undertaken against an information processing system or network does not fit under any of the traditional INTs. It typically has some connection with human intelligence (HUMINT), because it is often an extension of the technical collection efforts carried out by HUMINT operatives. Cyber collection also resembles communications intelligence (COMINT), especially when collection from data communications networks is involved. Collection against publically available information processing systems, such as the World Wide Web, falls in the category of open source.”*[27]

No official definition has emerged for cyber or cyber intelligence. They remain amorphous terms. [28]

Who Is in Charge?

As cyber intelligence has become vital to all of the other INTs, every organization is involved. The major players are NSA, CIA, and Cyber Command; others include DIA, NGA, FBI, DHS, other law enforcement entities, and a growing number of private cyber security/intelligence companies.

One former NSA official observed: “Whether Cyber should be an INT is mostly an organizational structure / management issue.”[29] In his textbook, Robert Clark wrote: “A structural debate exists... [O]ne view is that all offense (CNE and CNA) and cyber defense should be housed within the same organization.[30]

A consolidated approach was tried in 1981 when Admiral B.R. Inman, while still the Director of NSA (DIRNSA) and newly appointed as the Deputy DCI under William Casey, gave “sole control of computer-based intelligence” to NSA.[31]

Gus Hunt (CIA’s former chief technology officer) in an interview stated: “I think what you’re seeing ... is that people are asking the question are we appropriately structured or resourced and focused to be as effective as we possibly can in this new realm of cyber and cyber operations.”[32]

Yet, a unitary approach is not what the US is pursuing.[33] The recent law upgrading the National Programs Protection Directorate in DHS to the Cybersecurity and Infrastructure Security Agency (CISA) adds another major player to the mix.

The plethora of government organizations raises issues of coordination and resource allocations. The DoD and DHS budgets are different, overseen by separate Congressional committees. The FBI’s budget is under the Department of Justice. There are also differences between the National Intelligence Program (NIP) and the Military Intelligence Program (MIP). The variety of associated “turf” issues between missions and organizations, in both the Executive and Legislative Branches, works against both effectiveness and efficiency.

Legal and Policy Issues

It is not the focus of this article to delve into the myriad legal and related policy issues related to cyber and cyber intelligence. From a legal perspective cyber issues fall under Title 10 (Armed Forces) and Title 50 (War and National Defense of US Code, as well as Title 18 (Crimes and Criminal Procedure). In recent years, due to the revelations of Edward Snowden in 2013, controversies have surrounded the constitutionality and morality of cyber activities under the Foreign Intelligence Surveillance Act and Patriot Act and their amendments. As a result cyber operations have been modified and restricted.

Internationally, the fundamental policy issue is whether cyberattacks by a nation state could constitute an act of war. This became a NATO issue with the Russian cyberattacks on Estonia in 2007. “Broad access to cyberspace is so central to the strength of most nations today that cyber-based systems are considered critical national infrastructure and therefore, massive access shutdown or area denial operations could be considered acts of war, depending on the

[26] August 20, 2018 email from Larry Dietz, a professor at AMU citing a student’s paper.

[27] Robert M. Clark. *Intelligence Collection*. Washington D.C.: CQ Press, 2014, p 121.

[28] However, cyberspace and cyberspace exploitation, which mean much the same thing, have been defined in a military context. See JP 3-12, 8 Jun 2018, GL-4, *http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150*.

[29] July 23, 2018 email to the authors from Doug Price, former NSA official.

[30] Robert M. Clark. *Intelligence Collection*. Washington D.C.: CQ Press, 2014, p 140.

[31] Fred Kaplan, *Dark Territory*, New York: Simon & Schuster, 2016, p 27.

[32] *http://www.fifthdomain.com/*.

[33] It should be noted that some continue to argue for a unified approach. See Petraeus & Sridhar, “The Case for a National Cybersecurity Agency” 9/7/18. *https://www.politico.com/agenda/story/2018/09/05/cybersecurity-agency-homeland-security-000686?cid=apn* Page 3 of 77.

circumstances."[34] The Russian sponsored conflict in Ukraine is a prime example.

Observations and Conclusions

Cyberattacks are the #1 threat to the U.S. today, according to the DNI's 2018 threat statement to Congress. The major threat nation-states are Russia, China, North Korea, and Japan. Other states are also developing offensive cyber capabilities.[35]

Not only do cyber events happen at the speed of electrons flowing through networks, which makes reaction to cyberattacks difficult, such speed frustrates easy identification of the participants in an event. Experts have noted: "Cyberspace's manmade origin has resulted in three facets that distinguish it from the relatively consistent natural domains: complexity, adaptability, and rate of change... [C] yberspace is breathtakingly intricate and maddeningly nonlinear."[36] "The pace of change can be so abrupt as to render the conventional, action/reaction cycle of strategic evolution out of date before it has begun."[37]

Cyber intelligence has to anticipate potential attacks in order to alert intrusion detection triggering algorithms necessary for network defenses. With the quickly changing technological landscape and new vectors for adversary attacks, cyber intelligence must not only stay on top of software and hardware threats within the worldwide network environment but also draw from the background and threat intelligence provided by other INTs. In this regard cyber intelligence is a multi-intelligence fusion process as well as a cyber domain technical INT.

In his book, *The Future of Intelligence*, former Assistant DCI Mark Lowenthal writes: "... [T]he US intelligence community is made up of 'stovepipes,' that is verticals built either around an INT or based on which policy maker is an agency's principal client.... [S]ome organization has to be responsible for each INT – for managing collection systems, adjudicating priorities, processing, and exploiting the collected intelligence and disseminating it to the analysts who need it. Each INT is managed, collected, and processed somewhat differently, or vastly differently from the others... The INT stovepipes are not inherently bad as long as they do not create impediments."[38]

Arguing that cyber should be an independent INT, former J2 of the Joint Task Force for Computer Network Defense (JTFCND), Robert Gourley, drew a parallel with GEOINT:

> *"The IC established a new discipline called GEOINT, not because of new collection, there had always been imagery. And not because of analysis needs, there had always been all source analysis. But because a new world required a very special focus on intelligence analysis over terrain. It may well be that the intelligence community should treat the new world of cyberspace in a similar manner, establishing [CYBERINT] as a cross cutting discipline enabled by all the other elements of the IC, plus contributions from our network defenders, law enforcement, counterintelligence and of course open source. The result: A better ability to know what our adversaries are doing in cyberspace and a better ability to serve decisions makers at all levels of government, industry and among the general populace."*[39]

Gourley also noted that cyber intelligence "required deep connections into the counterintelligence and law enforcement world to learn everything we could about the adversaries in cyberspace."[40]

In describing MASINT, a relatively new INT in 2003, William K. Moore wrote:

> *"MASINT looks at every intelligence indicator with new eyes and makes available new indicators as well... [I]t can detect things that other sensors cannot sense, or sometimes it can be the first sensor to recognize a potentially critical datum."*[41]

Given the speed of cyber events, Moore's comment seems relevant to CYBERINT as well.

A major impediment to organizing cyber-related intelligence is the lack of definition of what it is and comprises. There is a wide divergence of opinions among involved professionals in various government departments and the private sector. Military experts view cyber as part of the information environment conflict, a competition that does not rise to the level of kinetic warfare, but is a conflict nonetheless.[42]

[34] Alison Lawlor Russell, "When Attackers Pull the Plug on the Internet," *Tufts Magazine* In Focus, *https://tuftsmagazine.com/in-focus/cyber-insecurity*. Russell is Professor of Political Science, Merrimack College, and author of *Cyber Blockades*, Washington, DC: Georgetown University Press, 2014.

[35] Testimony of Kevin Mandia, CEO of FireEye, Inc. before the United States Senate Select Committee on Intelligence, March 30, 2017. *CSPAN.org*.

[36] Col. Matthew M. Hurley, USAF. "For and from cyberspace: Conceptualizing cyber intelligence, surveillance, and reconnaissance," ISR Focus, *Air & Space Power Journal*, Nov-Dec 2012.

[37] Paul Cornish et al., "On Cyber Warfare," Chatham House Report (London: Chatham House [Royal Institute of International Affairs], November 2010), p 29. *http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf*. Cited by Hurley.

[38] Mark M. Lowenthal. *The Future of Intelligence*, Cambridge, UK: Polity Press, 2018, p 124.

[39] July 26, 2018 email to the authors.

[40] Gourley. Ibid.

[41] William K. Moore. "MASINT: new eyes in the battlespace." *Military Intelligence Professional Bulletin*, January–March 2003. Cited by Hurley.

[42] Comments of COL Jason Chung, USA, former G2, US Army Pacific, at the AFCEA TechNet Conference in Honolulu, Hawaii, November 14,

Turf issues abound. The US Government has taken a multi-organizational approach. The UK, by contrast, has centralized its cyber activities in the National Cyber Security Centre, a sub-organization of its NSA equivalent, the Government Communications Headquarters (GCHQ).

RAND analyst Martin Libicki once observed: "we generally first react by trying to jam the square peg of game-changing innovation into the round holes of the past."[43] Whether or not cyber intelligence should be a separate INT remains open to debate. But it definitely is a square peg that deserves more organizational thought.

The authors appreciate the thoughts, inputs and critique provided by Cynthia Storer. We would like to thank also those who were willing to share thoughts for this article, including John Allison, James Clapper, Lawrence Dietz, Rich Haver, Robert Gourley, Mark Lowenthal, Steve Marrin, Bill Nolte, and Doug Price. Reader's comments on this article are invited. Email *guide@afio.com*.

Robert M. Clark is an adjunct faculty member at Johns Hopkins University. He previously was a faculty member of the DNI's Intelligence Community Officers' Course and course director of the DNI's Introduction to the Intelligence Community course. Clark served as a USAF electronics warfare officer and intelligence officer. At CIA, he was a senior analyst and group chief for analytic methodologies. He is the author of *Intelligence Analysis: A Target-centric Approach* (6th edition, 2019), *The Technical Collection of Intelligence* (2010), and *Intelligence Collection* (2014). He is a co-author, with Dr. William Mitchell, of *Target-Centric Network Modeling* (2015) and *Deception: Counterintelligence and Counterdeception* (2018); and, co-editor, with Dr. Mark Lowenthal, of *Intelligence Collection: The Five Disciplines* (2015).

Peter C. Oleson is senior editor of *The Intelligencer, Journal of US Intelligence Studies* and Editor of AFIO's *Guide to the Study of Intelligence*. He is a former assistant director of DIA and the director for intelligence and space policy in the Office of the Secretary of Defense. He has been a faculty member of the DNI's Intelligence Community Officers' Course as well as at the National Defense Intelligence College, CIA University, the University of Maryland University College, and the University of Hawaii at Manoa. He is the editor of AFIO's *Guide to the Study of Intelligence* and numerous articles.

2018. Robert K. Ackerman, "Technology Underpins Indo-Pacific Command Intelligence," *Signal*, *https://www.afcea.org/content/technology-underpins-indo-pacific-command-intelligence*.

[43] Martin Libicki, "Cyberpower and Strategy." Remarks at the 8th International Institute for Strategic Studies Global Strategic Review, "Global Security Governance and the Emerging Distribution of Power," Sixth Plenary Session, 12 September 2010). Cited by Hurley.

SIGNIFICANT CYBER INCIDENTS 1997 - PRESENT

Incident	Comment
Eligible Receiver June 9, 1997 National Security Agency (NSA) "Red Team" hackers testing Department of Defense (DoD) systems.	The "entire defense establishment's network was penetrated – in four days." NSA's hackers also discovered "strangers" in DoD's networks – "traceable to French Internet addresses." [Review of *Dark Territory* by P. W. Singer, *New York Times*, Mar. 1, 2016.]
Solar Sunrise February 3, 1998 "Packet sniffer" was installed on a National Guard computer at Andrews AFB.	Malware was detected by the Air Force Information Warfare Center. Investigation led to two 16-year-old boys in California. [Fred Kaplan. *Dark Territory: The Secret History of Cyber War*. NY: Simon & Schuster, 2016.]
Moonlight Maze Early March 1998 Persistent hacker entered DoD networks via university research sites.	Time zone analysis pointed to Moscow. Honey pot[1] caught the Russian Academy of Sciences. Analysis showed commands had been typed in Cyrillic. JCS established the Joint Task Force Computer Network Defense (JTF-CND), the predecessor to CYBERCOM, the following July. [Kaplan, *Dark Territory*.]
Titan Rain Late 1990s – 2001… Chinese cyberattacks on US defense contractors.	Espionage related attacks to obtain weapons systems related data. In 2006 Chinese cyber espionage stole extensive documentation on the F-35 stealth fighter. [Kaplan, *Dark Territory*.]

[1] A honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems – Wikipedia.

Aurora Generator Test March 4, 2007 US Department of Energy test of attack on critical energy equipment.	Cyberattack caused a massive 27-ton 2.25-megawatt electrical generator to self-destruct. First experiment to determine that cyberattack could cause serious physical damage. [Kaplan, *Dark Territory*.]
Estonia April 27 – May 2007 **Massive Distributed Denial of Service[2]** **(DDoS) attack** May 8-9, 2007 Second wave of botnet attacks.	First large-scale use of cyberattacks by Russia against a neighboring state. Called “Web War One.” [*www.wired.com/2007/08/ff-estonia/*; Kaplan, *Dark Territory*.]
Georgia 8 August 2008 Broad DDoS and SQL injection attacks[3] cyberattacks accompanied Russian military intervention and seizure of the Georgian provinces of Ossetia and Abkhazia.	Cyberattacks accompanied Russian military intervention and seizure of the Georgian provinces of Ossetia and Abkhazia. Cyberattack rerouted the entire Internet in Georgia to Russian servers, which shut down Georgian sites. Georgian “mass media, finance, government ministries, police, and armed forces” hacked. Coupled with Russian propaganda offensive. [Kaplan, *Dark Territory*.]
Buckshot Yankee October 24, 2008 A worm detected by NSA in Central Command’s classified network.	A beacon attached to the worm[4] ‘agent.btz’ routed data to a foreign site. Within 24 hours NSA had ‘rerouted’ the beacon to an NSA site. Probably cause: someone in Afghanistan had inserted a contaminated thumb drive into the classified network. Russian supplied thumb drives were sold in Afghan kiosks. [Kaplan, *Dark Territory*.]
Operation Olympic Games Aka “STUXNET” 2010… An NSA developed super worm, “Flame,” infected Iranian nuclear program programmable logic controllers.	Probably developed about 2005, in conjunction with Israel, by 2010 STUXNET had damaged 25% of Iran’s centrifuges. STUXNET later became widespread affecting systems in Iran, Indonesia, India, Azerbaijan, Pakistan, the US, and others. [Symantec. “W32.Stuxnet,” September 17, 2010; Kaplan, *Dark Territory*.]
Saudi Aramco August 2012 Iranian cyberattack on Saudi Arabia’s national oil company.	“Shamoon” virus wiped out 30,000 hard drives at Saudi Aramco. Believed to be in retaliation for cyberattacks on Iranian National Oil Company earlier in 2012. [Kaplan, *Dark Territory*. Nicole Perlroth, “In Cyber Attack on Saudi Firm, US Sees Iran Firing Back,“ *New York Times*, Oct. 23, 2012.]
US Office of Personnel Management (OPM) 2012 – 2014 Breach of OPM database of SF-86 forms related to security clearance investigations.	Affected 22 million people. Significant compromise of national security. Hackers believed to be Chinese. [Taylor Armerding, *csoonline.com*, January 26, 2018.]
Rye, NY Dam Attack August – September 2013 Attempt to penetrate the Supervisory Control and Data Acquisition (SCADA) system of a flood control dam.	Iranian hackers accessed controls for a dam. [Scott E. Depasquale, “Power Plants and Transportation Systems Are at Risk,” *Tufts Magazine*, Fall 2018; Mark Thompson, “Iranian Cyber Attack,” *Time*, March 24, 2006; Max Kutner, Dam Hacking, *Newsweek*, March 30, 2016.]
Yahoo 2013 Data breach of email accounts and personal information.	Largest data breach to date, affecting 3 billion users. Breach was not reported until October 2017. [Fruhlinger, *csoonline.com*.]
Sands Corporation Attack February 10, 2014 Massive cyberattack attributed to Iran.	Target was Sands’ corporation chief, Sheldon Adelson, a vocal critic of Iran and supporter of Israel. [Kaplan, *Dark Territory*.]

[2] A Distributed Denial of Service (DDoS) attack uses many compromised computers (a “botnet” – a network of robot computers) to overwhelm an Internet site with attempts to connect that results in the targeted site crashing, thus denying legitimate users of the site access.

[3] SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server. – Wikipedia.

[4] A worm is a piece of self-replicating malware that adversely affects the operation of computer software and hardware.

Crimea February – March 2014 Integrated cyber, electronic warfare, and social media attack on Ukrainian province.	Used in conjunction with physical invasion by “little green men,” Russian spetnaz troops in unidentified uniforms of the Ukrainian province. [Kaplan, *Dark Territory*.]
Sony Pictures Entertainment November 24, 2014 North Korean malware attack in retaliation for the comedy movie The Interview about Kim Jung Un.	“Shamoon” wiper malware destroyed 3,000 of the company’s computers and 800 servers and 100 terabytes of digital records. [Kaplan, *Dark Territory*.]
Ukraine December 2015 Russian malware attack on Ukrainian power grid	Use of “KillDisk” malware. Viewed as testing for Russian cyberwar tactics. [Andy Greenberg. “The Untold Story of Notpetya, The Most Devastating Cyberattack in History,“ Security, Wired, Aug. 22, 2018.]
US 2016 election 2015 - 2016 Widespread Russian cyber and information warfare attack on US presidential election. Others trying to affect the election through cyber means were Qatar and the United Arab Emirates (UAE).	Most active Russian cyber entities were Advanced Persistent Threat (APT) 28 (Fancy Bear & Sofacy) and APT 29 (Cozy Bear), both elements of the GRU. Also active were troll farms of the “independent” Internet Research Agency). [Jane Mayer, “How Russia Helped Swing the Election for Trump: A meticulous analysis of online activity during the 2016 campaign makes a powerful case that targeted cyberattacks by hackers and trolls were decisive.” *The New Yorker. https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump?wpisrc=nl_cybersecurity202&wpmm=1.*]
United Kingdom Brexit Referendum June 2016 Russian use of cyber and social media to sow discord among UK voters.	More than 150,000 Russian Twitter accounts identified as promoting pro-Brexit votes. Unexplained crash of online voter registration site. [Joseph Hicks, “British Lawmakers Say Foreign States May Have Interfered in Brexit Referendum,” *Time*, April 12, 2017; David Kirkpatrick, “Signs of Russian Meddling in Brexit Referendum,” *New York Times*, November 15, 2017.]
Edward Snowden Leaks June 2016… NSA contractor fled Hawaii to Hong Kong and Russia and revealed to the press thousands of purloined NSA documents.	Snowden leaked a full fifty-page catalogue of tools and techniques used by NSA’s Tailored Access Office (TAO) – i.e., NSA’s hackers – that was published by *Der Spiegel*. [Kaplan, *Dark Territory*.]
Dyn attack, New Hampshire October 2016 DDoS attack	Attack knocked out Twitter, Netflix, PayPal and others in the eastern US and Europe. [Kaplan, *Dark Territory*.]
WannaCry May 2017 Ransomware attack that took over and encrypted hard drives until ransom paid in Bitcoin.	Major target was the UK’s National Health Service. [Josh Fruhlinger, CSO from IDG. *www.csoonline.com*]
NotPetya June – July 2017 Widespread Russian malware attack aimed at Ukraine that spread worldwide. [See box on opposite page on NotPetya]	“NotPetya infected millions of computers around the globe [and] is believed to be the costliest malware in history in terms of the damage it inflicted.” “Researchers with the cybersecurity firm ESET discovered links between the malware used to twice cut power in Ukraine and the NotPetya ransomware.” [FP Policy Brief, 10/15/2018. fp@*foreignpolicy.com*.]
Equifax July 2017 Criminal attack on database of credit reporting agency.	Breach affected 150 million people with Equifax accounts. [Fruhlinger. *csoonline.com*.]
GitHub February 2018 Massive DDoS attack	The largest DDoS attack recorded to date, possibly by Chinese hackers, utilizing an extensive botnet. [Fruhlinger. *csoonline.com*; Lily Hay Newman, “GitHub Survived the Biggest DDoS Attack Ever Recorded,” *Wired*, March 1, 2018.]

Iran Cyberattack on Iranian infrastructure and strategic networks October 2018 Unspecified but widespread attacks on Iran reported.	*Times of Israel* report "Israel silent as Iran hit by computer virus more violent than STUXNET." [*https://www.timesofisrael.com/tv-report-israel-silent-as-iran-hit-by-computer-virusmore-violent-than-stuxnet/*; Reuters, "Iran Accuses Israel of Failed Cyber Attack," November 5, 2018, *https://www.reuters.com/article/us-iran-israel-cyber/iran-accuses-is...failed-cyber-attack-idUSKCN1NA1LJ?wpisrc=nl_cybersecurity202&wpmm=1.*]
Marriott Hotels Cyber theft of massive Marriott data 2014 - 2018	Chinese MSS identified as perpetrators of the theft of individual travel information of approximately 500,000 Marriott customers. *New York Times*, Dec. 12, 2018.

Former US deputy national security advisor Tom Donilon in March 2013 said that China had unleashed an unprecedented scale of cyberattacks. Most active was PLA unit 61398.[5] China views the cyber domain as critical.[6] "China has become a bigger threat after a reorganisation of the People's Liberation Army (PLA) put hacking in the hands of contract firms, effectively privatising operations." "Free of previous Chinese state bureaucracy, they are run by computer science experts with extensive links into hacking forums and groups, says Crowdstrike, which provides cybersecurity for half of the world's biggest 20 multinationals."[7]

[5] Kaplan, *Dark Territory*, p 221.

[6] Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2018, Office of the Secretary of Defense, May 16, 2018, p 74-5.

[7] Charles Hymas. China is ahead of Russia as 'biggest state sponsor of cyber-attacks on the West,' *The Telegraph*, 9 October 2018. *https://www.telegraph.co.uk/technology/2018/10/09/china-ahead-russia-biggest-state-sponsor-cyber-attacks-west/?WT.mc_id=tmg_share_em*.

NOTPETYA – THE COSTLIEST CYBERATTACK TO DATE[1]

It started with a cyberattack on the Linkos Group, a company in Kiev, Ukraine, which sent updates to accounting software (M.E.Doc – akin to TurboTax or Quicken), by "Sandworm," a Russian hacking group. They hijacked Linkos' update servers to allow a hidden back door into the thousands of PCs around the Ukraine and the world that have M.E.Doc installed. Then, in June 2017, the saboteurs used that back door to release a piece of malware called "NotPetya," their most vicious cyber weapon yet. The code was honed to spread automatically, rapidly, and indiscriminately. "NotPetya was propelled by two powerful hacker exploits working in tandem: One was a penetration tool known as 'EternalBlue,' created by the US National Security Agency but leaked in a disastrous breach of the agency's ultrasecret files earlier in 2017." "NotPetya's architects combined that digital skeleton key with an older invention known as 'Mimikatz.'" "[F]rom hospitals in Pennsylvania to a chocolate factory in Tasmania. It crippled multinational companies, including [the shipping giant] Maersk; pharmaceutical giant Merck; FedEx's European subsidiary, TNT Express; French construction company Saint-Gobain; food producer Mondelez; and manufacturer Reckitt Benckiser. In each case, it inflicted nine-figure costs. It even spread back to Russia, striking the state oil company Rosneft." In the Ukraine "[o]n a national scale, NotPetya was eating Ukraine's computers alive. It would hit at least four hospitals in Kiev alone, six power companies, two airports, more than 22 Ukrainian banks, ATMs and card payment systems in retailers and transport, and practically every federal agency."

The result was more than $10 billion in total damages, according to a White House assessment: Maersk - $250-300m, Merck $870m, TNT Express $400m. "[I]t was the equivalent of using a nuclear bomb to achieve a small tactical victory," Tom Bossert, former White House Homeland Security advisor, said. "Global corporations are simply too interconnected, information security too complex, attack surfaces too broad to protect against state-trained hackers bent on releasing the next world-shaking worm."

[1] Andy Greenberg. "The Untold Story of NotPetya, The Most Devastating Cyberattack in History," Security, *Wired*, Aug. 22, 2018. *https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world*.