AMERICAN INTELLIGENCE JOURNAL

THE MAGAZINE FOR INTELLIGENCE PROFESSIONALS

Cyber Security and Operations

NMIA

2010

Treasure Trove or Trouble:
Cyber-Enabled Intelligence and International Politics

by Dr. Chris Bronk, Rice University

Oft-mentioned in the lore of U.S. intelligence is the quip of former Secretary of War and State, Henry Stimson, who offered the belief, "Gentlemen don't read each other's mail," as explanation for closing the State Department's code-breaking cryptanalytic office, the Black Chamber, in 1929. Dismissed as error by the Chamber's director, Herbert Yardley, as a naïve mistake, intercepting, decrypting, and capturing information remains a fundamental component of the intelligence enterprise. Nearly a century after the closing of Yardley's office, much has changed in communications technology, but the idea that mass connectivity through cyberspace to enormous repositories of information somehow changes the larger political and ethical issues surrounding intelligence collection is a red herring. Nation-states can, and will continue to, collect information regarding strategic dispositions and intentions in their quest for security. As Microsoft's trustworthy computing chief Scott Charney argues, "It is important to recognize that military espionage has been occurring from time immemorial, and that some victims of military espionage may be engaged in such espionage activities themselves."[1]

Decades of technological advancement notwithstanding, the U.S. Intelligence Community (IC) is wise to embrace this reality, continue to develop the enhanced operating picture produced by Information Technology (IT), and construct pragmatic, interdisciplinary mechanisms and practices designed to protect information resources and at the same time maintain the capacity to purloin foreign-held information of benefit to national security. What this does not mean is that there shall be no rules in cyberspace for government or the IC. On the contrary, cybercrime and malicious acts designed to subvert critical systems should be thwarted at every possible opportunity. In addition, the IC should respect intellectual property protected by copyright, patent, and trade secret. Maintaining these positions while accepting the realities of contemporary global interactions—a post-Cold War, post-9/11, post-Internet world—will not be easy, but it should be accepted that doctrine regarding the cyber domain of intelligence is not written on a blank slate. In cyber intelligence, the sources and methods are markedly changed, but that does not mean that the macro issues regarding intelligence collected by the cyber channel cannot be liberally borrowed from other domains.

A REVOLUTION IN AWARENESS

The Internet has changed intelligence. As Joseph Nye and ADM William Owens (USN, Ret)—the former a respected Harvard professor and former Clinton administration Defense Department official and the latter a former Vice Chairman of the Joint Chiefs of Staff—argued over a decade ago, "The one country that can best lead the information revolution will be more powerful than any other."[2] The widely recognized experts asserted this for good reason. Through application of IT, principally the networking of personal computers to one another across global distances, the United States has markedly changed the information picture provided to both top leaders and field operatives across the span of government.

Information technologies permit the United States to extend the sharp end of its political reach around the globe. A footnote from the ongoing operations against Al Qaeda is an exemplar in this case. In November 2002, Ali Qaed Senyan al-Harthi, aka Abu Ali, a suspect in the 2000 bombing of the USS *Cole* in Aden, was killed along with five other individuals as they rode in a vehicle 125 miles east of Sana'a, Yemen's capital. A laser-guided missile fired from a CIA-directed Predator destroyed their vehicle.[3] The loop of intelligence collection to action exemplified by the attack on Abu Ali has been repeated numerous times since, with UAVs used regularly in attacking terror suspects in Afghanistan, Iraq, Pakistan, and elsewhere.

Across global distances, in real time, intelligence is collected, analyzed, and transformed into policy involving the use of force. We have learned in the last decade that meshes of sensors, networked computers, and distributed nodes of intelligence may be employed to more effectively wage war in either symmetric or asymmetric conflicts. One lesson is clear: the combatant more adept at employing its information resources and connecting them to action increases its chances to prevail. But what if those information resources are unavailable, stolen, or manipulated? Returning to Predator, the platform used to

successfully conduct the strike against Abu Ali, it was revealed in 2009 that the vehicle's image signal data were being transmitted unencrypted in the clear and therefore open to intercept by anyone sophisticated enough to capture them.[4] This epitomizes the double-edged sword that is intelligence in a time of mass information.

UNDERSTANDING THE VULNERABILITY

For all of the different modalities of cyber-attack, worms, viruses, bots, and other pieces of technical vernacular, outcomes of a cyber-attack can generally be divided into one of three categories: (1) systems are rendered unavailable; (2) the integrity of the system is compromised; and/or (3) confidentiality of information is compromised.[5] Despite the rich technical context, policy requires transcribing the latest exploit or attack into one of the three categories above. The type of attack manifests itself in markedly different outcomes. If a system's operational capacity is degraded or it is entirely knocked offline, its users are quite typically painfully aware of that fact. On the other hand, data breaches or integrity attacks, in which unauthorized actors gain access to protected systems, may go undetected for weeks, months, or even years. Attacks headed under integrity and confidentiality should be of concern to the IC, both on the offense and defense.[6]

In thinking of where national security and cybersecurity intersect, perhaps instructive is a visit to the 1983 Turing Lecture given by the co-recipient of the highest award bestowed by the Association of Computing Machinery (ACM), Ken Thompson, then an employee of Bell Labs and now on staff at Google. Recognized for his work in the development of the UNIX operating system, Thompson took the opportunity to illustrate his own efforts to subvert trusted computer code by creating a Unix C compiler that would create a backdoor in the programs it modified from human readable text to binary code optimized for processing. This permitted an unauthorized user with knowledge of the back door to gain access and, thus, trusted use of the system. The vulnerability could be located only by auditing the compiled code in binary form, something far less readable than the original source written in the C language.[7]

Thompson's backdoor indicates the potential for cyber vulnerabilities across all systems, including those built, bought, and used by government.[8] Like other large organizations, the U.S. Department of Defense and the rest of the federal bureaucracy use productivity and operating system software produced by commercial developers. Fiscally, it would be inherently foolish for the U.S. government to write its own productivity software[9] and, with a record of failure in tweaking commercial available products or building its own,[10] the open market often prevails for good reason.

Imperfect and vulnerable systems underpin national strategy reliant on information awareness delivered by computer, both in the United States and elsewhere. While the most specialized of military computing platforms, such as those in fighter aircraft and submarines, may still be purpose-built to the most rigorous of specifications, the information management applications used in command and control are typically derived from commercial products.[11] This presents an easy answer to one question in cyber espionage: attack the fighter's computer system, or the inventory management system for its spares and armaments? One can be reasonably sure that the logistical system likely runs on something similar to what is openly available on the market. It is also worth noting that the development tools used to build the custom military software bits all run on standard OS platforms. It may be more efficacious to skip trying to hack the jet and instead hack the workstation used to program the jet's software.

INTELLIGENCE AND THE EVOLVING FACE OF DIGITAL BATTLE

Decision rests with the practitioner of cyber intelligence to determine which systems of his adversary are most easily exploited and may represent the greatest potential payoff. Being able to read an adversary's critical communications is certainly of enormous value, as it was during those windows in which the cryptographic mechanisms trusted by the warring powers of the 20th century failed them without their knowing.[12] But also of use is the ability to create a composite picture from ancillary systems outside the military organization itself.[13] Simply seeing the FedEx or phone bill for an organization will yield important clues with regard to its operations and planning.[14] The difficulty is in creating the mechanism in pooling this less valuable data and processing in a meaningful way.

Vulnerability of cyber-infrastructure to intrusion is largely a product of the original design parameters of the first digital, packetized network, ARPANET, and its adoption as the architecture of the contemporary Internet. In 1988, a self-replicating piece of software, a *worm*, released by a Cornell graduate student, Robert Tappan Morris, exposed the great vulnerability of the system that would become the Internet. Two decades later, the Internet largely remains an open system that has had layers of security grafted onto it to facilitate trusted transactions and communications. Developers of the Internet espoused a value set found in science: like scholarship, digital information should be transmitted across an open architecture, readily accessible with minimal obstruction.[15] This value remains overlain

upon the many protocols, hardware, and user applications to transmit massive amounts of data, from e-commerce transactions, email, and web pages to video, telephone calls, and government communications.

In a manner recognizable to practitioners of electronic warfare, in the cyber domain malicious measure should be met with a commensurate countermeasure. Viruses must be met with anti-virus software, spam e-mail with spam filters, spyware agents with anti-spyware programs, and on. Thwarting damage to networked computers is largely an exercise in collecting all of the known information regarding malicious software code (the particular signatures of viruses, worms, Trojans, bots, and whatever the hacker community invents next) and being prepared to meet it.[16] While variations of known threats may be profiled and defeated, stability in information security may be upset by innovation, and often is. As such, this technical environment is one that lends itself to the attacker, whether a sole operator, transnational group, or nation-state. The attacker generally has an advantage, because the attacker only needs one hole to get through, and it does not matter where it is.

POLITICAL ESCALATION: ELECTRONIC JOYRIDERS TO PEER COMPETITORS

Individuals, groups, or national governments may perpetrate cyber-attacks. The borderless, boundary-free geography of cyberspace holds a fluidity in which traditional mechanisms for expression of state sovereignty and international law are awkwardly out of place.[17] A contemporary stereotype reinforced in film, the sole hacker is often cast as a warrior of mythic potential, who by himself or herself can enter combat with large, monolithic institutions and win. Closer to reality is the view of hacker as skill set,[18] as an individual able to gain unauthorized access to or disrupt the function of networked computer systems which may operate independently, confederate with others, or hold allegiance to a government.

For those on the receiving end of a cyber-attack, the difficulty is determining attribution, which remains a formidable obstacle. Even when a determination of the source of attacks designed to either knock systems offline or purloin their digital content may be mapped across the Internet, sovereignty has limits. Botnets, networks of compromised "zombie" computers employed by nefarious actors to launch cyber-attacks, may be spread across dozens of countries, considered both friend and foe. The family PC in Seoul or San Francisco may be an email spam platform, zombie denial-of-service bot, or node of an intelligence collection system.

CYBER INTELLIGENCE ≠ CYBERWAR

For it to be cyberwar, it must first be war," argues Bruce Schneier. However, agreement in the security community on this assertion is hardly complete.[19] Certainly, network attacks would be highly useful tools in the information operations component of any state-versus-state conflict. If one party can disrupt command and control of, collect intelligence about, and generally confuse the other, it is hard to imagine why it would not do so, but the thorny question arises when such attacks cross the line of business as usual in intelligence collection and move across the divide to conflict. As many as a hundred nation-states have developed information warfare capabilities, either defensive or offensive or both.[20] But what sort of an information attack is an act of war?

Discussion on that front takes us to the April-May 2007 cyber-attacks launched against Estonia after the country moved a Soviet-era monument to its unknown soldiers of the Great Patriotic War from central Tallinn to a military cemetery. The Estonia cyber-attacks were covered extensively in the media, and an official of the defense ministry "compare[d] the attacks to those launched against America on September 11th 2001."[21] A NATO official raised a tough question as the Estonia attacks, which brought large pieces of the government, financial, and news media's digital infrastructure to a grinding halt, progressed. "If a member state's communications centre is attacked with a missile, you call it an act of war. So what do you call it if the same installation is disabled with a cyber-attack?"[22] Such a conundrum begs for opinion from international law with special attention to types of attack and their outcomes, but it is unclear how much of this problem is applicable to the issue of intelligence collection.

THE GEOPOLITICS OF DIGITAL ESPIONAGE

While details of cyberwarfare incidents remain debated and incomplete, any list of nations representing considerable future potential in the cyber conflict domain would likely hold the People's Republic of China in one of its top three or four slots. Profoundly influenced by their observation of the U.S.-led coalition's actions in the war with Iraq in 1991, Chinese military scholars continue to refine concepts of what they now label "integrated network electronic warfare."[23] Such thinking has worked its way up to the highest levels of government in the PRC, with Jiang Zemin stating in his report to the 16th Party Congress in 2002, "Efforts should be made to accomplish the historical tasks of mechanization and *IT application*, thereby bringing about leapfrog development in the modernization of our army."

Although the People's Liberation Army has obvious interest in mirroring the IT-driven force multiplier capabilities of the United States,[24] it is also interested in collecting information by electronic means about those organizations which threaten its security. Often, when data theft takes place, a finger is pointed at the PRC and the PLA. Network intrusions at the U.S. Defense and State Departments, Congress, and elsewhere have been conjectured to be the exploits of the Chinese government or its digital proxies. In the summer of 2008, the Obama presidential campaign's network was penetrated, with FBI and Secret Service officials describing "a problem way bigger than what you understand." According to the report, federal agents asserted to Obama staffers, "You have been compromised, and a serious amount of files have been loaded off your system."[25] Likely culpable was a "foreign entity,"[26] with one newspaper announcing after election day, "US government cyber investigations have determined that an attack this summer on the Obama and McCain campaign computer networks originated in China."[27]

Allegations of cyber-attacks invariably link back to China, and an increasing body of work confirms those linkages. GhostNet, a cyber counterespionage activity conducted by Canadian academics and technologists, indicates that penetrations of networks in more than one hundred nations were likely overseen by an entity within the People's Republic of China.[28] Indeed, the focus of GhostNet's attention was the IT supporting the Dalai Lama and other Tibetan organizations. And GhostNet is just one item in a long list of allegations against the PRC in collecting intelligence via networked computer. Google's allegation of theft in January 2010 of the company's intellectual property by Chinese operatives prompted the company to pull up stakes for its Google.cn search portal and shift traffic to its Hong Kong operation.

Although China certainly appears to be investing heavily in its cyber capabilities, not least those designed to purloin sensitive information, one may be reasonably certain that the U.S. government also holds an enormous cyber-espionage capability as well.[29] Setting aside the allegations of warrantless, dragnet-style wiretapping by the National Security Agency, there is evidence that the United States' cyber-espionage capability has held a significant role in the formulation of foreign policy. Consider David Sanger's *New York Times* article, "U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site." Sanger attributes the decision not to permit an Israeli attack on Iran to a U.S. Intelligence Community (IC) report asserting that Iran had discontinued its nuclear weapons program in 2003. How was that conclusion reached? Buried halfway in the piece was the statement, "The assessment, a National Intelligence Estimate, was based on a trove of Iranian reports obtained by penetrating Iran's computer networks." If Sanger's source is to be believed, information regarding Iran's cessation of activity to weaponize enriched uranium may have come from tapping into the computers of its nuclear researchers.

Such news indicates that the world's major powers are employing tools to collect intelligence from computer networks. As copying digital information is an exercise of relative ease, and network penetration remains possible despite the best efforts of some in government and a still-growing information security industry, the theft of digital data will likely continue to be a growth area. The question for the IC will be how to exploit this opportunity while at the same time not inhibiting the overall security of cyberspace.

Notes

[1] Charney, Scott, *Rethinking the Cyber Threat - A Framework and Path Forward*, Microsoft, p. 10.
[2] Nye, Joseph, and William Owens, "America's Information Edge," *Foreign Affairs*, March/April 1996, p. 24.
[3] Monaghan, Elaine, and Daniel McGrory, "Death of terror chief deals severe blow to al-Qaeda," *The Times (London)*, November 5, 2002.
[4] Anderson, Nate, "Predator drones use less encryption than your TV, DVDs," *Ars Technica*, December 17, 2009, available online at http://arstechnica.com/tech-policy/news/2009/12/predator-drones-use-less-encryption-than-your-tv.ars.
[5] *An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12*, National Institute of Standards and Technology, October 1995.
[6] What the IC should defer to matters of war and peace are those attacks that knock systems offline, potentially threatening civilian life.
[7] Thompson, Ken, "Reflections on Trusting Trust," *Communications of the ACM*, August 1984, Vol. 27, No. 8.
[8] The author sets aside the matter of air-gapping regarding networks which do not touch the larger global Internet in this article.
[9] For more detailed discussion, see Abts, Christopher, *COTS Software Integration Modeling Study*, Century for Software Engineering, University of Southern California, June 1997.
[10] See May, Lorin, "Major Causes of Software Project Failures," *Crosstalk: The Journal of Defense Software Engineering*, July 1998, and Charette, Robert, "Why Software Fails," *IEEE Spectrum*, September 2005.
[11] Indeed, some 78% of the hardware and 76% of the software used in the Virginia-class nuclear-powered attack submarine are COTS. *USS Virginia Class C3I System*, Lockheed Martin Corporation, 2003, available online at http://www.lockheedmartin.com/data/assets/1082.pdf.
[12] Kahn, David, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, New York: Scribner, 1996.
[13] Steele, Robert, *On Intelligence: Spies and Secrecy in an Open World*, Fairfax, VA: AFCEA, 2000.

[14] This is sometimes called "traffic analysis" and is referred to as "chatter" by those in the intelligence field. Knowing who is chatting with whom, in what volume, can represent valuable intelligence.
[15] Leiner, et. al., "A Brief History of the Internet," *ACM SIGCOMM Computer Communication Review*, 39(5), October 2009.
[16] Christodorescu, Mihai, and Somesh Jha, "Testing Malware Detectors," *ACM SIGSOFT Software Engineering Notes*, 29(4), July 2004.
[17] Joyner, Christopher, and Catherine Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework," *European Journal of International Law*, Vol. 12, No. 5, 825-865.
[18] Bronk, Chris, *In confidence: Information technology, secrecy and the state*, Ph.D. dissertation, Syracuse University, 2005.
[19] "Marching off to cyberwar," *The Economist*, December 6, 2008, p. 20.
[20] CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*, CSIS, December 2008.
[21] "A cyber riot," *The Economist*, May 10, 2007.
[22] "A cyber riot," *The Economist*, May 10, 2007.
[23] *Annual Report: Military Power of the People's Republic of China 2009*, U.S. Department of Defense, 2009, p. 14.
[24] Richard Bitzinger, "China's 'Revolution in Military Affairs': Rhetoric Versus Reality," *China Brief*, Jamestown Foundation, 8(5).
[25] "Hackers and spending sprees," *Newsweek*, November 5, 2008, available online at http://www.newsweek.com/id/167581.
[26] "Obama, McCain campaigns' computers hacked for policy data," CNN, November 6, 2008, available online at http://www.cnn.com/2008/TECH/11/06/campaign.computers.hacked/index.html.
[27] Sevastopulo, Dimitri, "Chinese hack into White House network," *Financial Times*, November 6, 2008.
[28] "Tracking Ghostnet: Investigating a Cyber Espionage Network," *Information Warfare Monitor*, 2009.
[29] Bronk, Chris, "Webtapping: Securing the Internet to Save Us from Transnational Terror?" *First Monday*, 13(11).

Christopher Bronk is the Baker Institute Fellow in Technology, Society, and Public Policy (TSPP) and a lecturer in Rice University's Department of Computer Science. He previously served as a career diplomat with the U.S. Department of State on assignments both overseas and in Washington, DC. His last assignment was in the Office of eDiplomacy, the Department's internal think tank on information technology, knowledge management, computer security, and interagency collaboration. He also has experience in political affairs, counternarcotics, immigration, and U.S.-Mexico border issues. Since arriving at Rice, Bronk has divided his attention among a number of areas including information security, broadband policy, Web 2.0 in government, and the militarization of cyberspace. He has provided commentary for a variety of news outlets including ABC, The Wall Street Journal, *NPR, and the BBC. Holding a Ph.D. from the Maxwell School of Syracuse University, Bronk also studied international relations at Oxford University and received a bachelor's degree from the University of Wisconsin-Madison.*

American Intelligence Journal

THE MAGAZINE FOR INTELLIGENCE PROFESSIONALS

Vol. 28, No. 2 *2010* ISSN 0883-072X

The *American Intelligence Journal* (*AIJ*) is published by the National Military Intelligence Association (NMIA), a non-profit, non-political, professional association supporting American intelligence professionals and the U.S. Intelligence Community, primarily through educational means. The Board of Directors is headed by Lieutenant General James A. Williams (USA, Ret), and the president of NMIA is Colonel Joe Keefe (USAF, Ret). NMIA membership includes active duty, former military, and civil service intelligence personnel and U.S. citizens in industry, academia, or other civil pursuits who are interested in being informed on aspects of intelligence. For a membership application, see the back page of this *Journal*.

Authors interested in submitting an article to the *Journal* are encouraged to send an inquiry – with a short abstract of the text – to the Editor by e-mail at <William.Spracher@dia.mil>. Articles and inquiries may also be submitted in hard copy to Editor, c/o NMIA, 256 Morris Creek Road, Cullen, Virginia 23934. Comments, suggestions, and observations on the editorial content of the *Journal* are also welcome. Questions concerning subscriptions, advertising, and distribution should be directed to the Production Manager at <Admin@nmia.org>.

The *American Intelligence Journal* is published semi-annually. Each issue runs about 100 pages and is distributed to key Government officials, members of Congress and their staffs, and university professors and libraries, as well as to NMIA members, *Journal* subscribers, and contributors. Contributors include Intelligence Community leaders and professionals as well as academicians and others with interesting and informative perspectives. Back issues of the *AIJ* are available to members within the U.S. at the cost of $25; to non-members and international requestors at $50.