Intelligence Preparation of the Information and Communications Environment

By Jeffrey Carr

While the Joint Intelligence Preparation of the Operational Environment (JIPOE) is for offensive purposes, this paper proposes a role for what the author has called the Intelligence Preparation of the Information and Communications Environment (IPICE) which, if implemented, will improve defensive tactics by commercial as well as governmental entities. The components of IPICE can be reversed and applied in an offensive manner against a foreign target however that's a topic for a different paper.

The current trend among information security companies is "intelligence-driven security". Lockheed Martin may have pioneered the concept thanks to the work of their employees like Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin who wrote the paper "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains"[1]. Cloppert later created a very detailed model for APT attacks[2] which led to his above-referenced paper and which RSA liberally borrowed from in their paper "Getting Ahead of Advanced Threats: Achieving Intelligence-Driven Information Security".[3]

Today, Lockheed Martin's model is being widely used among members of the Defense Industrial Base (DIB) and the DOD's Defense Cyber Crime Center which feeds threat intelligence to the DIB. In fact, Lockheed recently won a contract[4] worth over $400 million to provide digital forensics and analysis support to DC3. While this system works well for the purpose intended, it represents an inadequate view of the overall threat landscape. This is due in large part to the security vendors who support the DIB and most of the Fortune 500 with their cyber security solutions; solutions that have both limited effectiveness against targeted attacks and a very narrow scope of a company's operational environment.

Before a private corporation or the federal government can evaluate the effectiveness of any cyber security process, especially something called "intelligence-driven", it's necessary to have a complete view of the threat landscape or operating environment of the organization. Lockheed Martin's Intrusion Kill Chain only looks at typical APT-styled attacks that rely on spear phishing with email attachments, spear phishing that encourages the reader to click on a malicious link, and malicious payloads delivered via removable media. Advocates of this approach say that it represents the majority of attacks that they see. The objective of this paper is to lay out a more comprehensive picture of the threat landscape by using the DOD's Joint Intelligence

Preparation of the Operational Environment (JIPOE).[5] The JIPOE can serve as an effective model for crafting a comprehensive Information and Communication Technology (ICT) security plan based not upon the current narrowly defined threatscape (i.e., Lockheed Martin and RSA's intrusion kill chain) but upon a more complete operational picture. The following is an abridged outline of the JIPOE as described in Joint Publication 2-01.3:

First Step of JIPOE: Defining the Operational Environment

- Identify the Operational Area
- Determine the Significant Characteristics of the Operational Environment
- Determine Intelligence and Information Gaps

Second Step of JIPOE: Describe the Impact of the OE

- Develop a Geospatial Perspective of the OE
- Develop a Systems Perspective of the OE

Third Step of JIPOE: Evaluating the Adversary

- Update or Create Adversary Models
- Determine the Current Adversary Situation
- Identify Adversary Capabilities and Vulnerabilities

Fourth Step of JIPOE: Determining Adversary Courses of Action

- Identify the adversary's likely objectives and desired end state
- Identify the full set of adversary's COAs

I've simplified the above steps from four to three being:

1. Define the Attack Surface (i.e., Operational Environment)
2. Evaluate the Adversary
3. Determine Adversary Courses of Action

What is "Intelligence"?

The word intelligence in the phrase "cyber intelligence" is confusingly used by the information security industry and the media. Sometimes it's used interchangeably with malware data. Other times it's used to describe open source investigations into Anonymous and other hackers. The word "Cyber" has its own definitional issues so for the purpose of this paper, the author recommends Nicolas Eftimiades', author of "Chinese Intelligence Operations"[6] definition which is actually more of an informal description of the traditional intelligence process:

> "Intelligence agencies worldwide share the same overall goal: to provide accurate and timely intelligence to their consumers. To do so they collect raw information from a variety of human and technical sources. They must then collate and analyze that data to separate fact from fiction and make judgments about a variety of past, current, and future

> events. The completed analytical product, intelligence, is then disseminated to the consumer, whose information requirement started the process. That person or group is then in a position to ask for additional analysis or to implement policy based on the intelligence received. The entire process is known as the intelligence cycle."

The Attack Surface

A Multinational Corporation (MNC) has a vast attack surface. Before an effective security framework can be constructed, the attack surface needs to be established. The information environment of a corporation, government, or military organization includes both internal and external threats. The Insider Threat, meaning a hostile action taken against the company by an employee, is an active and often unreported problem for many companies and one that usually costs more than than breaches by outsiders.[7] Another form of Insider Threat is what happens when a company hires foreign engineers to staff their R&D offices in China, Russia, France, and other nations. While at employed at the company, these engineers learn proprietary information that they take with them when they resign to work for a state-run company with similar interests in another year or two. This is known as "Technology-Transfer".

External threats include far more attack vectors than just those used by APT-styled attacks. They include but aren't limited to:

- Company offices outside of the United States that are subject to foreign ICT laws on information collection can have all of their communications legally intercepted and monitored. This includes email, VOiP, mobile, landline, satellite and VPN.
- Multinational Corporations may be required to provide their source code to foreign intelligence services for inspection to ensure that it doesn't pose a threat to their national security. Failure to comply would mean being stopped from doing business within that country's borders.
- Company employees, particularly executives, who have their devices compromised when traveling overseas.
- Foreign vendors who the company engages for contract work may have affiliations with their native government and upon request pass trade secrets to that government thanks to their authorized access on the U.S. company's network.
- Vendors' subcontractors, subsidiaries, and/or strategic partners may have affiliations with their native government and do the same as above.

Evaluate The Adversary

There are over 28 nation states[8] who are standing up cyber warfare/espionage capabilities. Many of them have known relationships with hacker groups and a growing number are standing up volunteer militias who are trained to operate in cyberspace. While Russian[9] and Chinese[10] capabilities have been extensively documented, India's National Security Council have assigned authorities for offensive cyber operations to the Defense Intelligence Agency and the National Technical Research Organisation[11]. Israel's Military Intelligence Unit 8200 and its C4I Directorate have both announced a recruitment drive among Israel's elite hackers[12]. Currently the following countries are standing up commands equivalent to or based upon U.S. Cyber Command: Australia, Brazil, Bulgaria, Canada, China, Czech Republic, Estonia, Finland, France, Georgia, Germany, India, Iran, Israel, Italy, Myanmar, Netherlands, North Korea, Pakistan, Poland, Romania, Russia, Singapore, South Africa, South Korea, Sweden, Taiwan, Ukraine and Zimbabwe. Of these, the most active States engaging in cyber espionage attacks by state and non-state actors are Brazil, Bulgaria, China, France, Georgia, india, Iran, Israel, Netherlands, North Korea, Romania, Russia, South Korea, Taiwan and Ukraine. U.S. multinational companies that have offices in these states should consider their networks already breached and be taking appropriate steps to mitigate the effects of that state.

Foreign Intelligence Services Legal Authorities

Both Russia and China have enacted laws which allow their respective security services a great deal of latitude in collecting information from foreign corporations who maintain offices within their borders. A survey of what those laws mean for foreign companies is provided below, however it doesn't stop with just Russia and China. India has been aggressively pursuing similar tactics and other countries have their own policies and procedures. The Security Operations Center and Chief Counsel of every MNC should be aware of the impact that these authorities have on their company and their sensitive data.

State Security Law of the People's Republic of China

The State Security Law of the People's Republic of China (PRC) governs how China's security services may operate and mandates the participation of its population if asked. In other words, if you're a visitor staying at a hotel in Shanghai, the staff of that hotel must cooperate with any request by the security service to give them access to your room without your knowledge or consent if presented as an issue of state security. Here are some relevant portions of the law, which can be found in full at china.org. cn:

Article 8 Any functionary of a State security organ may, when carrying out a task for State security, enter any interested site upon producing an appropriate certificate, and may, in accordance with the relevant provisions of the State, with approval and upon producing an appropriate certificate, enter interested restricted areas, sites or units; and may have access to related files, materials, and articles for examination.

Article 10 Where the reconnaissance of an act endangering State security requires, a State security organ may, in accordance with the relevant provisions of the State and after going through strict approval procedures, employ technological means of reconnaissance.

Article 11 Where State security requires, a State security organ may inspect the electronic communication instruments and appliances and other similar equipment and installations belonging to any organization or individual.
Article 16 Citizens and organizations shall provide convenience or other assistance for the work of State security.

Article 18 When a State security organ investigates and finds out any circumstances endangering State security and gathers related evidence, citizens and organizations concerned shall faithfully furnish it with relevant information and may not refuse to do so.

Russian Federation Federal Law No. 40
The Russian version of the above Chinese law is known as Federal Law No. 40 "On The Federal Security Service (FSB)". The original law was passed in 1995 with the latest amendment passed in 2008. Chapter II Article 8 sets out the FSB's main authorized activities. They are:

- counterintelligence activities;
- combating terrorism;
- combating crime;
- intelligence activities;
- border activities;
- ensuring information security.

Information security is seen as a primary, not a subsidiary, activity. The next several articles lay out more detail on each specific activity, often with implications for information security. For example, counterintelligence activities include the authority to monitor communications. Indeed, measures to secure information through monitoring and collection activity figure prominently throughout the articles. Note that the FSB is authorized to conduct intelligence activity, specifically foreign intelligence activity, even though Russia maintains a separate Foreign Intelligence Service (SVR). The law states that foreign intelligence operations are done on the basis on joint agreements with the SVR.

Article 11.2 sets outs the details for information security activity. They are:

- the formation and implementation of public and scientific-technical policy in the field of information security, including the use of engineering and cryptographic means;
- providing cryptographic and engineering methods of security for information and telecommunications systems, and systems encrypted, classified, and other types of special communications in Russia and Russian agencies located outside Russia.

In short, FSB information security authority is extremely broad. They set both administrative and technical policy. The FSB effectively runs Russia's cryptographic infrastructure with authority over software and hardware. Indeed, Article 3 places Russia's Academy of Cryptology, nominally an academic institution, under the Federal executive authority for security, the FSB. FSB implementing regulations specifically state that the FSB operates the Academy of Cryptology. Implementing regulations, signed by then President Putin, provide additional details giving the FSB authority to regulate development, import, sale, and export of cryptographic technologies. The implementing regulations also allow the FSB to assist organizations in protecting commercial secrets.

Under Article 15, public authorities as well as enterprises, institutions, and organizations are obliged to provide assistance to the Federal Security Service in carrying out their assigned duties.

Individuals and legal entities in Russia that provide postal services and telecommunications of all kinds, including systems, data communication, and confidential satellite communications, are obliged at the request of the Federal Security Service to include extra hardware, equipment, and software, as well as create other conditions necessary for the operational and technical measures by the Federal Security Service.

In order to meet the challenges of RF, security forces of the Federal Security Service can be assigned to public authorities, enterprises, institutions, and organizations irrespective of ownership, with the consent of their managers in the manner prescribed by the president of Russia, leaving their military service. In other words, if the FSB asks for your help, you help. If they ask you to modify hardware or software to so they can execute an operation or monitor a network, you do it. And if they want to place someone if your organization to support FSB objectives, they can do so with your management's permission.

The implementing regulations include provisions not specifically mentioned in the law. For example, the FSB is allowed to establish banks and deal in foreign exchange. The FSB conducts research and development, and manufactures technology independently and with “other businesses, institutions, and organizations”, including the information security field. Significantly, these provisions hold for all FSB activities, not just information security. For example, the FSB could instruct a company, including a software exporter, to modify that software to assist an FSB technical collection operation. The FSB could form a covert company and sell tailored software directly over the internet taking payment in foreign exchange. Indeed, aggressive FSB use of provisions found in the FSB law and regulations presents a significant threat only limited by the FSB’s objectives and imagination.

Determine Adversary Courses of Action

Thanks to ongoing global innovations in information and communications technology, there is no way to identify every possible attack vector but known courses of action broadly include social engineering, spear phishing, software exploits, hardware backdoors, ICT intercepts, and insider threats. Every commercial, governmental, and military organization needs to be aware of each of those attack vectors and have a plan in place to counter them.

Notes

[1] Hutchins, Eric M., Cloppert, Michael J., Amin, Rohan M., “Intelligence-Driven Computer Network Defense Informated by Analysis of Adversary Campaigns and Intrusion Kill Chains”, Proceedings of the 6th International Conference on Information Warfare, Spring 2011.

[2] “Security Intelligence: Defining APT Campaigns” http://computer-forensics.sans.org/blog/2010/06/21/security-intelligence-knowing-enemy/

[3] “Getting Ahead of Advanced Threats: Achieving Intelligence-Driven Information Security” by RSA, based upon discussions with the Security for Business Innovation Council

[4] Lockheed Martin To Assist Department Of Defense In Fight Against Growing Threat: Cyber Crime”: PR Newswire, May 3, 2012

[5] Joint Publication 2-01.3, The Joint Chiefs of Staff, U.S. Department of Defense. http://www.fas.org/irp/doddir/dod/jp2-01-3.pdf

[6] Eftimiades, Nicholas (2011-02-19). Chinese Intelligence Operations (Kindle Locations 169-173). Naval Institute Press. Kindle Edition.

[7] US-CERT “Interesting Insider Threat Statistics”, October 25, 2010: http://www.cert.org/blogs/insider_threat/2010/10/interesting_insider_threat_statistics.html

[8] 28 States are surveyed in Chapter 16 of Inside Cyber Warfare 2nd Edition (O’Reilly, 2011), however additional States have added those capabilities in 2012. Eventually every nation with an Armed Forces will also have something akin to the U.S. Cyber Command..

[9] “Inside Cyber Warfare: Mapping the Cyber Underworld” 2nd edition, chapter 15 “The Russian Federation: Information Warfare Framework”, 12/2011

[10] USCC, “"Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage", 2012: http://www.uscc.gov/

[11] http://www.theregister.co.uk/2012/06/11/india_state_sponsored_attacks/

[12] http://www.jpost.com/Defense/Article.aspx?id=253487

Jeffrey Carr

Jeffrey Carr is the founder and CEO of Taia Global, Inc. and is the author of “Inside Cyber Warfare: Mapping the Cyber Underworld” (O’Reilly Media 2009 and 2011 (2nd edition)). His book has been endorsed by General Chilton, former Commander USSTRATCOM and the Forward to the second edition was written by former Homeland Secretary Michael Chertoff. Jeffrey has had the privilege of speaking at the US Army War College, Air Force Institute of Technology, Chief of Naval Operations Strategic Study Group, the Defense Intelligence Agency, the CIA’s Open Source Center and at over 60 conferences and seminars.