CSIS/DOJ Active Cyber Defense Experts Roundtable
March 10, 2015

On March 10, 2015 the Center for Strategic and International Studies, in conjunction with the Cybersecurity Unit of the U.S. Department of Justice (Criminal Division), convened a group of leading private sector cybersecurity practitioners for a roundtable discussion regarding a field of cyber defense that some have called "active cyber defense."[1] The meeting was part of the Cybersecurity Unit's ongoing efforts to gather information about techniques that the private sector is (and is not) using to protect its networks in a heightened cyber threat environment.

What follows is a summary of the major topics discussed and the views expressed by the private sector participants during that meeting.[2]

Issue 1: The Scope of "Cyber Defense." Recently there has been much public debate about measures that companies can lawfully take to protect their computer networks and data. The discourse has at times been hindered by the use of varying, overlapping, or confusing terminology. What is the best nomenclature to define the scope of activities that companies conduct to protect their networks?

1. The cybersecurity practitioners agreed that the phrase "defensive cyber actions" best describes the current state of network security activities.

   a. "Defensive cyber actions" captures the full range of activities conducted for purposes of network defense, which could be characterized as including an array of activities from intelligence gathering to actions taken in response to a cyber threat that may impact a remote network.

   b. "Defensive cyber actions" was also preferred over "active defense."

   c. At least one practitioner strongly disfavored the term "countermeasures" as that implies an offensive intrusion onto other networks (so-called "hacking back"), which does not accurately represent current security efforts.

[1] A representative from the National Security Division of the Department of Justice also attended the session.
[2] The views expressed herein are those of the private sector participants and not the Department of Justice or the United States government.

Issue 2: Cyber Intelligence Gathering as Cyber Defense Activity. Cyber defense activities encompass a range of tools and techniques, from preventive measures intended to prevent or deter malicious cyber activity to actions taken in response to a particular, ongoing cyber threat. Where does gathering cyber intelligence fall in this spectrum?

1. The practitioners stated that cyber intelligence gathering is a vital component of defensive cyber actions.

    a. They explained that cyber intelligence gathering provides information on the adversary's targeting, tools, infrastructure, tactics, and procedures. This information can then be used to gird against future activity. Such intelligence gathering can also provide information about the type and quantity of information stolen from a company that is used for purposes of conducting a damage assessment.

    b. In general, the practitioners expressed that cyber intelligence gathering can be conducted by lawful monitoring of the infrastructure commonly used by intruders, such as "hop points," to store exfiltrated data.

Issue 3: Lack of Legal Certainty. Because defensive cyber actions can raise a variety of issues (e.g., concerning privacy laws and electronic surveillance statutes), private sector practitioners may consult their lawyers before conducting some types of defensive cyber activity. How do current cyber laws affect network security operations?

The practitioners explained that legal uncertainty—either in the law itself, or in the interpretation of the law by counsel—can thwart the implementation and timeliness of defensive cyber actions, even when conducted on one's own network.

1. They explained that counsel are reluctant to authorize some types of network monitoring, even when user consent has seemingly been obtained to such monitoring, or where there is no obvious legal bar.

    a. For instance, there is a reluctance to conduct monitoring of devices connected to a network of a company that has implemented a "bring your own device" policy.

        i. Some company lawyers have also expressed reservations over the use of other helpful intelligence gathering activities in the "dark web," such as participation (or even mere presence) in discussions in hacker chat rooms.

    b. In particular, in-house attorneys who are uncomfortable with electronic surveillance laws may be reluctant to authorize monitoring, even when seemingly adequate consent for monitoring has been obtained.

    c. Some of these reservations may be driven by concerns over public perception rather than purely legal concerns.

2. They also expressed that the current state of substantive laws such as the Computer Fraud and Abuse Act ("CFAA") and some privacy statutes can adversely affect network security operations.

    a. It is important to analyze actions taken on customer data separately from actions taken on corporate network data, given the differing legal and privacy interests.

    b. There is also some concern that some types of network scanning that rely on executing an exploit to determine whether a vulnerability exists (*e.g.*, the "Heartbleed" vulnerability) may violate the CFAA.

3. The practitioners reported that "sinkholing" (e.g., re-registering domain names used for malware command-and-control servers) is common and effective, but raises concerns because, unless appropriate precautions are taken, the new owner may begin receiving data from computers in other victim networks, including those of business competitors.

<u>Issue 4: Conducting Defensive Cyber Action in a Global Environment</u>. The largest companies often have a global presence with networks located in multiple countries and may need to comply with various different legal regimes. Even smaller companies may encounter similar problems if they rely upon cloud computing. How do international jurisdictional issues affect defensive cyber actions?

1. The practitioners explained that statutory requirements may vary from country to country, and the laws and practices of some countries pose particular challenges.

    a. Sometimes, companies have built special localized systems to comply with a country's requirements such as data privacy standards.

    b. In "BRIC" countries (Brazil, Russia, India, and China), there may be special rules that U.S. companies must follow that can affect their ability to implement defensive cyber actions.

    c. In China, the government is proposing that companies share their encryption keys and install backdoors for government use.

2. The practitioners added that for multinational companies, certain privacy laws and standards are a major factor affecting implementation of defensive cyber actions. The EU Data Privacy laws are a particular source of difficulty.

a. They said that a single company monitoring its own network may need to use multiple user agreements drafted to address the disparate laws of several countries in a single region.

b. They also said that disparity in the legal requirements and privacy laws of different countries has inhibited the use of cyber threat indicators in a cloud computing environment. Some cyber threat indicators may be considered "personally identifiable information" (PII) in some countries thereby complicating the process of using the indicators in cloud computing architecture.

i. Practitioners said there should not automatically be an assumption that PII should be removed from data used for network defense purposes. PII is also sometimes helpful and necessary for network defense reasons.

<u>Issue 5: "Hacking Back</u>." More aggressive defensive cyber actions—sometimes called "hacking back"—have been central to the ongoing legal and policy debate over measures that companies should and should not be permitted to conduct in defense of their networks and data. What is the current state of cyber activities conducted outside one's network, including punitive actions?

1. The practitioners explained that defensive cyber actions are rarely conducted to retrieve stolen data. They further clarified that –

a. "Web bugs" and "beacons" are only sometimes used to find stolen data; when they are used, it is usually in connection with unsophisticated intruders because such measures are easily detected and thwarted by a sophisticated actor.

b. To the extent that stolen data is traced to hop points and accessed by victim companies or their agents, such access is typically used to generate cyber threat intelligence or to help with a damage assessment rather than for purposes of retrieving stolen data. Retrieving stolen data is ordinarily thought to be technically impractical because of the limited time frame in which exfiltrated data would need to be accessed and deleted or encrypted.

c. Companies will sometimes use legal process or the cooperation of an ISP to address stolen information that they have located on a remote server. Streamlining such process would be helpful in retrieving data under these circumstances.

d. The most common scenarios for obtaining the credentials for accessing a hop point involve capturing the credentials in plain text during a File Transfer Protocol session or finding the credentials hard-coded into malware.

2. The practitioners said that self-deleting or self-encrypting technology is not in broad use and may not even be feasible.

    a. Before considering something as sophisticated as this technology, the practitioners recommended that companies identify their "crown jewels," or critical assets, and focus on better protecting them.

    b. They believe that most companies do not know what their critical assets are and, therefore, are not well positioned to properly protect the data on their networks.

3. The practioners stated that activities that "impose costs" on intruders have some value, but only a limited range of activities were identified as productive.

    a. They said botnet takedowns and other coordinated malware eradication activities are examples of imposing costs with commensurate benefits.

    b. They noted that direct action against an attacker, including "hacking back," could lead to unintended consequences, such as escalation by the attacker who may misinterpret the source and intent of such actions.

Issue 6: Effective Cyber Defense Actions. The spectrum of activities that can be initiated to protect a network and data is broad. What cybersecurity actions are most effective?

1. The practitioners suggested that traditional security measures are often effective against more common threat actors; therefore, the rigorous application of such measures should be considered a best practice. Against particularly sophisticated or advanced threat actors, however, they suggested using cyber intelligence gathering as an additional component of a defensive program.

2. Some also suggested that greater law enforcement-private sector cooperation would be the most effective step toward increasing overall cybersecurity going forward.