Lab Note

CYBER TECHNOLOGY

Training the Cyber Defensive Line

A game-like competition is helping build experts in cyber "disaster response."

The number of attacks on computer networks is massive; for example, in 2013, the Pentagon reported getting 10 million attempted cyber intrusions a day.[1] These attacks are also growing in sophistication, primarily because cyber attackers are using combinations of techniques such as inserting malicious code (malware) or email phishing, and are adding complexity to the attack by involving multiple parties.[2] And, cyber intruders are breaching systems in just minutes.[2] Network operators, who are typically tasked with day-to-day maintenance of the computer systems, are hard-pressed, and often not trained, to address this flood of advanced, novel attacks.

In response to the proliferation and growing complexity of cyber threats, the U.S. Cyber Command (USCYBERCOM) over the last three years has created squads who will act as cyber "strike teams" in the field to protect the nation's networks. To help the Department of Defense (DOD) build such cyber protection teams, staff from Lincoln Laboratory's Cyber Security and Information Sciences Division, in collaboration with several other federally funded research and development centers (FFRDC) and university-affiliated research centers (UARC), developed and conducted a series of exercises designed to evaluate the capabilities of cyber defenders. Not exactly games, these exercises, collectively called Project C, pit a red team attacking the network against a blue team defending it. The red team plans an attack strategy, and the blue team develops countermeasures to thwart the attack. "The blue team needs to learn about the network and how best to defend it, locate any attacks, defeat them, and, finally, redefend the network," says Douglas Stetson, associate leader of the Laboratory's Cyber System Assessments Group.

Project C's primary goals are to assess and improve the performance of cyber teams and to advance technologies for cyber ranges (i.e., virtual environments for training cyber analysts and developing cyber defense tools). "Physical bodies are not the solution alone," according to Lee Rossey, former leader of the Cyber System Assessments Group, who helped establish Project C. "You need the methodology and the tools." Rossey likens an effective cyber team to a football team: each player has a role, and they've all read the playbook and understand

---

1 B. Fung, "How many cyberattacks hit the United States last year?" *National Journal*, 8 March 2013, available at http://www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/.

2 "Verizon 2015 Data Breach Investigation Report Finds Cyberthreats Are Increasing in Sophistication; Yet Many Cyberattacks Use Decades-Old Techniques," PRWire, 15 April 2015, available at http://www.prnewswire.com/news-releases/verizon-2015-data-breach-investigations-report-finds-cyberthreats-are-increasing-in-sophistication-yet-many-cyberattacks-use-decades-old-techniques-300066005.html.

the team's offensive and defensive strategies. To develop a cyber playbook, Project C researchers are investigating a number of questions: What makes one cyber team more successful than another? Why is one set of defenses more effective than another? How can we improve a team's capabilities? Answers to these questions will ultimately direct researchers to ways for improving subsequent rounds of training.

Project C sessions are conducted to help members of cyber protection teams be prepared to assist agencies undergoing serious cyber attack. How quickly a cyber team should be deployed to a site depends on two factors: the severity of the incident and and the asset under attack. While an intrusion accomplished by a lone hacker most likely is handled expeditiously by an in-house computer security group, a coordinated assault by "well-armed" cyber adversaries requires highly trained, cyber security rapid responders. Because the DOD cannot constantly defend all data on its systems, the department has created a three-tiered Prioritized Defended Asset List for key missions and systems on a given network. Cyber teams are called in more quickly for higher-priority assets that are critical to the government's continued functioning than for lower-ranked systems. Rossey also notes that "just because a network goes down, it doesn't mean that you're under attack."

A Project C exercise is a multiday event. At the start of each day's session, the staff members leading the exercise give participants a full briefing on the Project C format; the red team gets an additional briefing on their attack scenarios. The "battle" typically runs from 8:00 a.m. to 1:00 p.m. Before the red team begins its attacks, the blue team patches all known operating system (e.g., Windows 7) errors so that teams do not have to consider those errors when devising their stratagems. To make the exercise for the blue team is as real as possible, the red team typically generates four to six different attacks derived from real-world threats detailed in Verizon's Data Breach Investigations Report (available on request from http://www.verizonenterprise.com/DBIR/). The blue team must ensure that their defensive actions preserve the integrity, confidentiality, and availability of all data. As the blue team works to mitigate threats, the red team is figuring out the blue team's strategies, and when one type of attack is defended, the red team tries another.

Noncombatant teams, called white teams, monitor the process, give advice if necessary, and score the results (number of successful and unsuccessful attacks, number of attacks identified by the blue team, mitigation results). Red team attack actions, blue team actions (even those not correlated to an attack), chat logs, network traffic, and other data are collected throughout the session, and a summary out-briefing is conducted in the afternoon. The five-hour multi-attack exercise, which in reality would be a situation spanning a few days, is fast-paced and stressful. In the out-briefing, blue team interactions resulting from the pressurized exercise (e.g., inadequate communication, heated discussions) are analyzed because the team dynamics are as important to the successful resolution of attacks as are the expertise and tools the team brings to the conflict.

One significant advantage Project C has over other serious gaming scenarios used in DOD cyber defense training is that it can simulate any of the various government networks and communication environments, such as ShoreNet for naval ships, warfighter communications in the field, power-grid-management networks, or command-and-control systems for the

nation's missile defense systems. Project C allows cyber teams to work within a notional network-connected environment nearly identical to the real one they may be asked to defend. This virtual network environment, enabled by the Laboratory's LARIAT and K0ALA tools[3], includes all important elements, such as servers, users, and network activity.

Another advantage of Project C is that it is scalable and adaptable to different levels of attack severity and sophistication and to any type of network. The 2013 Defense Science Board (DSB) Task Force Report on Resilient Military Systems and the Advanced Cyber Threat classifies various types of cyber attackers. These cyber invaders range from individuals with commonplace equipment who simply employ malware developed by others to nation states that have the ability to execute cyber attacks that employ clever, new tactics. These classifications characterized in the DSB report also reflect the level of felonious intent of the perpetrators. Less malicious hackers break into networks for the challenge of doing so. Others invade systems seeking data that they can sell (e.g., the government's proprietary technical information). Critical threats to the United States are attackers targeting information that may give their nation states a military advantage. Project C's scalability and adaptability make it a valuable tool for improving the skills of respondents to all these types of attackers. It also provides an opportunity for participants to try out innovative cyber security technologies.

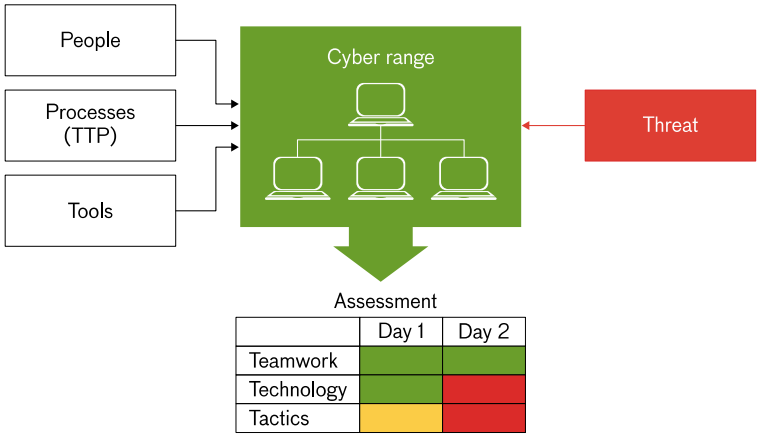
Experience gained by the researchers from Lincoln Laboratory, colleagues from FFRDCs and UARCs, and the Project C participants is being applied to the future strategy for training cyber protection teams. With guidance from the Laboratory's technical staff, the DOD held evaluation exercises last summer to compare the skills of three teams who had undergone a five-week Project C–type pilot training program in April and May to the skills of teams that had not engaged in such red team/blue team exercises. Analysis of the summer 2015 assessment sessions will be used to inform the direction of USCYBERCOM's cyber defense training. You might say Lincoln Laboratory is helping draft the playbook for the DOD's cyber protection defensive line.

Blue team members analyze traffic and logs to determine whether an attack has occurred against their network. More than 60 personnel from active-duty, reserve, and guard units

[3] For more information about these tools, see the article "Advanced Tools for Cyber Ranges" in this issue of the *Lincoln Laboratory Journal*.

assigned to USCYBERCOM's cyber protection forces participated in the Project C exercises conducted at Lincoln Laboratory.

During the exercises, observers watch the cyber range activity and follow how blue team players respond to cyber incidents, gauging the effectiveness, creativity, and speed of the measures deployed to counter the red team attacks.



Project C sought to assess the people, processes, and tools of the cyber protection teams in a realistic environment with a realistic threat. The Project C format provides a day-by-day evaluation of how the team members interacted, how their technology worked, and how effective their tactics, techniques, and processes (TTP) were. In the "stoplight" evaluation chart, green indicates a highly successful performance; yellow, a satisfactory performance; and red, a breakdown or failure in performance.