

# *Journal of Homeland Security and Emergency Management*

---

*Volume 7, Issue 1*

2010

*Article 74*

---

## **Live Fire Exercise: Preparing for Cyber War**

**Kenneth Geers**, *Naval Criminal Investigative Service and  
the Cooperative Cyber Defence Centre of Excellence*

**Recommended Citation:**

Geers, Kenneth (2010) "Live Fire Exercise: Preparing for Cyber War," *Journal of Homeland Security and Emergency Management*: Vol. 7 : Iss. 1, Article 74.

**Available at:** <http://www.bepress.com/jhsem/vol7/iss1/74>

**DOI:** 10.2202/1547-7355.1780

©2010 Berkeley Electronic Press. All rights reserved.

# Live Fire Exercise: Preparing for Cyber War

Kenneth Geers

## Abstract

In May 2010, the Cooperative Cyber Defence Centre of Excellence and the Swedish National Defence College hosted the Baltic Cyber Shield (BCS) international cyber defense exercise (CDX). For two days, six Blue Teams from northern European government, military and academic institutions defended simulated power generation companies against a Red Team of 20 hostile computer hackers. The scenario described a volatile geopolitical environment in which a hired-gun Rapid Response Team of network security personnel defended Critical Information Infrastructure (CII) from cyber attacks sponsored by a non-state terrorist group. This article covers the origin and evolution of CDXs, and it describes the design, goals and lessons learned from BCS 2010.

**KEYWORDS:** cyber defense exercise, CDX, cyber attack, Baltic Cyber Shield, Blue Team, Red Team, hacker, Estonia, Sweden

## 1. Introduction: the CDX concept

Many national security thinkers fear that the age of cyber terrorism and cyber warfare is coming soon. And the target list seems to grow by the day: electricity,<sup>1</sup> water, air traffic control, stock exchange,<sup>2</sup> national elections,<sup>3</sup> and more. However, the extent to which cyber attacks pose a real threat to national security is unclear. Expert opinions range from dismissive<sup>4</sup> to apocalyptic.<sup>5</sup>

We do know that there are worrisome trends in information technology (IT). National critical infrastructures are increasingly connected to the Internet. At the same time, their custom IT systems, some created in the 1950s and 1960s, are now being replaced with less expensive, off-the-shelf and Internet-enabled Windows and UNIX systems that are not only easier to use but easier to hack. The older systems were relatively more secure because they were not well-understood by outsiders, and because they had minimal network contact with other computer systems (Preimesberger, 2006).

National security planners require a better understanding of the threat posed by cyber attacks as soon as possible. Some real-world case studies exist.<sup>6</sup> However, much information lies outside the public domain, there have been no wars yet between two Internet-enabled militaries, and the ignorance of many organizations regarding the state of their own cyber security is alarming. Looking toward the future, military planners must be able to simulate cyber attacks and test cyber defenses within the bounds of a safe, laboratory environment, without threatening the integrity of operational networks.<sup>7</sup>

---

<sup>1</sup> The threat to electricity encompasses everything that relies on electricity to function, including computer systems. In May 2009, President Obama stated that “cyber attacks have plunged entire cities into darkness” (White House), reportedly referencing large scale, anonymous attacks in Brazil (CBS, 2009).

<sup>2</sup> In May 2010, after the Dow Jones surprisingly plunged almost 1,000 points, White House adviser John Brennan stated that officials had considered but found no evidence of a malicious cyber attack (Wagner, 2010).

<sup>3</sup> In 2007, California held a hearing for election officials on the subject of whether hackers could subvert the integrity of the state’s touch-screen voting machines. While the system manufacturer disputed the validity of the tests, the RT leader testified that the voting system was vulnerable to numerous attacks that could be carried out quickly (Orr, 2007).

<sup>4</sup> Persuasive cyber war skeptics include Cambridge University Professor Ross Anderson, *Wired* “Threat Level” Editor Kevin Poulsen, and *Foreign Policy* editor Evgeny Morozov.

<sup>5</sup> In early 2010, former U.S. Director of National Intelligence Michael McConnell testified that the U.S. would “lose” a cyber war today, and that it will probably take a “catastrophic event” before needed security measures are undertaken to secure the Internet (Bliss, 2010).

<sup>6</sup> This author has highlighted the cases of Chechnya, Kosovo, Israel, China, and Estonia (Geers, 2008).

<sup>7</sup> Occasionally, “penetration tests” are conducted against operational networks, but extreme care is always taken to avoid denial-of-service and/or the loss of sensitive data.

The need for cyber defense exercises (CDX) is clear. But the complex and ever-changing nature of IT and computer hacking makes conducting a realistic CDX an enormous challenge, and may render its conclusions valid only for a short period of time. The world is experiencing a rapid proliferation of computing devices, processing power, user-friendly hacker tools, practical encryption, and Web-enabled intelligence collection.<sup>8</sup> At the same time, a CDX requires the simulation of not only adversary and friendly forces, but even the battlefield itself.

Of course, the military is no stranger to computers. Software is now used to train tank drivers and pilots; it is also used to simulate battles, campaigns, and even complex geopolitical scenarios. But it remains controversial how closely a computer simulation can model the complexity of the real world. Myriad factors can contribute to failure: poor intelligence, incorrect assumptions, miscalculations, a flawed scoring system, and even political considerations. In 2002, the U.S. military spent \$250 million on a war game called Millennium Challenge, which was designed to model an invasion of Iraq. In the middle of the exercise, the Red Team (RT) leader, Marine Corps Lt. Gen. Paul Van Riper, quit the game on the grounds that it had been rigged to ensure a Blue Team (BT) victory (Gomes, 2003).

This article covers the origin and evolution of CDXs, and it describes the design, goals, and lessons learned from a recent “live-fire” international CDX, the May 2010 Baltic Cyber Shield (BCS). BCS was managed at the Cooperative Cyber Defence Centre of Excellence (CCD CoE) in Tallinn, Estonia. Its virtual battlefield was designed and hosted by the Swedish Defence Research Agency (FOI) in Linköping, Sweden with the support of the Swedish National Defence College (SNDC).<sup>9</sup> Over 100 participants hailed from across northern Europe.

## 2. CDX design

A robust CDX requires a team-oriented approach. There are friendly forces (Blue), hostile forces (Red), technical infrastructure (Green), and game management (White). The RT and BTs are the CDX combatants. The Green Team (GT) and White Team (WT) are non-combatants; RT attacks against either in most CDXs are strictly prohibited.

BT personnel are normally real-life system administrators and computer security specialists. Their goal is to defend the confidentiality, integrity, and availability (CIA) of their computer networks against hostile RT attacks. In BCS

---

<sup>8</sup> In the Internet age, Open Source Intelligence Collection (OSINT), against both people and organizations, is easier and more powerful than ever.

<sup>9</sup> The Estonian Cyber Defence League, Finland’s Clarified Networks, NATO Computer Incident Response Capability - Technical Centre (NCIRC-TC), Sweden’s Civil Contingencies Agency (MSB) and National Defence Radio Establishment (FRA) also participated in the CDX.

2010, the BTs were the primary targets for instruction; their progress was tracked by an automated and manual scoring system.

The RT plays the role of a cyber attacker, or in this CDX, a “cyber terrorist.” The RT attempts to undermine the CIA of BT networks using a variety of hacker tools and tactics.<sup>10</sup> In a “white box” test, RTs may be given detailed, prior knowledge of the BT networks; a “black box” test requires the RT to gather this information on its own.<sup>11</sup> Either way, RTs – just like real-life hackers – have an enormous advantage over their BT counterparts: they can often methodically work their way through various cyber attacks until they succeed in hacking the network.<sup>12</sup>

The WT manages and referees the CDX. Normally, it writes the game’s scenario, rules, and scoring system. The WT will make in-game adjustments in an effort to ensure that all participants are gainfully employed throughout the CDX. It also seeks to prevent cheating: for example, if a particular firewall rule appeared to be detrimental to the game and/or unrealistic in real-life, the WT may disallow it. Finally, the WT often declares a CDX “winner.”

The GT is responsible for designing and hosting the CDX network infrastructure. It is the in-game “Internet Service Provider” (ISP). To allow for post-game analysis, the GT should attempt to record all CDX network traffic. With the aid of virtual machine technology, it is technically possible to carry out a CDX on a handful of computers, but to simulate a powerful adversary, significant resources are required, and a time- and labor-intensive CDX is unavoidable (the RT, for example, should have a plan that indicates the availability of significant money and manpower). With Virtual Private Network (VPN) technology, the RT, BTs, and WT can be located anywhere in the world and remotely connect to the CDX environment. All automatic scoring in the CDX is implemented by the GT.

### 3. CDX goals

Cyber warfare is very different from traditional warfare. Tactical victories amount to a reshuffling of the electronic bits of data – also known as ones and zeros – inside a computer. At that point, an attacker must wait to see if any intended real-

---

<sup>10</sup> In the U.S., Sandia National Laboratories have developed eight “natural categories” of Red Teaming: design assurance, hypothesis testing, benchmarking, behavioral Red Teaming, gaming, operational Red Teaming, penetration testing and analytic Red Teaming (Preimesberger, 2006).

<sup>11</sup> A black box is often considered more realistic, because real-world hackers normally find themselves in this position. However, given strict time limits, white box CDXs are the norm. In BCS 2010, the RT had access to the initial BT network for three weeks prior to the CDX.

<sup>12</sup> In a CDX, this depends in part on the complexity of the network the BTs have to defend, and the amount of time the RT has to attack it. In the real world, hackers can often remain anonymous in cyberspace, so deterring cyber attacks is difficult. Attackers may be able to keep trying to crack a network until they succeed, and there is normally no penalty for the failed attempts (Geers, 2010).

world effects actually occur. A cyber attack is best understood not as an end in itself, but as an extraordinary means to a wide variety of ends: espionage,<sup>13</sup> denial of service,<sup>14</sup> identity theft,<sup>15</sup> propaganda,<sup>16</sup> and even the destruction of critical infrastructure.<sup>17</sup>

The primary goal of a CDX is to credibly simulate the attack and defense of a computer network. At the tactical level, the RT has the same goals as any real-world hacker, to gain unauthorized access to the target network.<sup>18</sup> If “administrator” or “root” access is obtained, the intruder may be able to install malicious software and erase incriminating evidence at will. Further actions, possibly aimed to support some political or military goal, could range in impact from a minor annoyance to a national security crisis.

The CDX “scenario” is helpful in determining the overall strategic significance of an exercise. A well-written scenario should estimate the required resources and projected cost of a theoretical attack. This in turn helps national security planners to determine whether a person, group, or nation could attempt it. For example, it still remains difficult to imagine a lone hacker posing a threat to a nation-state.<sup>19</sup> However, future cyber attacks might change that perception.

It is almost impossible for a limited-duration CDX to simulate the threat posed by a nation-state. Military and intelligence agencies are “full-scope” actors, which do not rely solely on computer hacking to achieve an important objective. Governments draw from a deep well of expertise in many IT disciplines, including cryptography, programming, debugging, vulnerability discovery, agent-based systems, etc (Lam et al, 2003). Those skill sets are in turn supported by experts in

---

<sup>13</sup> The most famous case to date is “GhostNet,” investigated by *Information Warfare Monitor*, in which a cyber espionage network of over 1,000 compromised computers in 103 countries targeted diplomatic, political, economic, and military information (“Tracking GhostNet...,” 2009).

<sup>14</sup> During a time of domestic political crisis, hackers were able to knock the entire nation-state of Kyrgyzstan offline (Keizer, 2009).

<sup>15</sup> American identities and software were reportedly used to attack Georgian government websites during its 2008 war with Russia (Gorman, 2009).

<sup>16</sup> Since the earliest days of the World Wide Web, Chechen guerilla fighters have demonstrated the power of Internet-enabled propaganda (Goble, 1999). On a lighter note, a hacker placed a series of fake articles on the USA Today website. One read, “Today, George W. Bush has proposed ... a Cabinet Minister for Propoganda and Popular Enlightenment [sic]... if approved, Bush would appoint Dr. Joseph Goebbels to the post” (“USA Today’ Website Hacked...” 2002).

<sup>17</sup> Department of Homeland Security (DHS) officials briefed CNN that Idaho National Laboratory (INL) researchers had hacked into a replica of a power plant’s control system and changed the operating cycle of a generator, causing it to self-destruct (Meserve, 2007).

<sup>18</sup> There are exceptions, such as a denial-of-service attack in which the main goal is to overload the system with superfluous data.

<sup>19</sup> Nonetheless, it is astonishing what some lone hackers have been able to accomplish. In 2001, “mafiaboy”, a 15 year-old from Montreal, was able to deny Internet service to some of the world’s biggest online companies, causing an estimated \$1.7 billion in damage (Verton, 2002).

the natural sciences, physical security, supply chain operations, continuity of business, social engineering,<sup>20</sup> and many more.

The Sandia National Laboratories RT, based in New Mexico, provides a robust model. Sandia has a long track record of successfully hacking its clients, which include military installations, oil companies, banks, electric utilities and e-commerce firms. Its RT takes pride in finding hidden vulnerabilities in complex environments, including obscure infrastructure interdependencies in highly specialized domains (Lawlor, 2004).<sup>21</sup> A former Sandia RT leader put it best: “Our general method is to ask system owners: ‘What's your worst nightmare?’ and then we set about to make that happen” (Gibbs, 2000).

#### 4. CDX history

Every CDX is unique. There are simply too many variables in cyberspace, and IT continues to evolve at an astonishing rate. Some CDXs are conducted only in a laboratory, while others take place on real networks in the real world. For the latter, cyber defenders may be warned about the CDX before it starts, or the RT attack may come as a complete surprise.

In 1997, an RT of thirty-five U.S. National Security Agency (NSA) personnel, playing the role of North Korean hackers, targeted the U.S. Pacific Command from cyberspace. The CDX, code-named Eligible Receiver, was an enormous success. James Adams wrote in *Foreign Affairs* that the RT was able to infect the “human command-and-control system” with a “paralyzing level of mistrust,” and that “nobody in the chain of command, from the president on down, could believe anything” (2001). Furthermore, Eligible Receiver was credited with revealing that a wide variety of national critical infrastructures was equally vulnerable to common hacker tools and techniques (Verton, 2003).

Many CDXs involve a proof-of-concept. In 2006, the U.S. Environmental Protection Agency asked the Sandia RT to conduct a vulnerability assessment of every water distribution plant serving at least 100,000 people. The fear was that a malicious hacker might be able to change the chemical composition of water enough to poison it. When the RT discovered that there were 350 such facilities in the country – far too many to examine each one – Sandia decided to conduct a thorough analysis of five sites, and then to construct the Risk Assessment Metho-

---

<sup>20</sup> Social engineering takes advantage of human weaknesses in security. Experience shows that malicious or co-opted insiders, due to the physical access they have to IT systems, can do more damage to an organization than a malicious outsider (Lawlor, 2004). This type of attack can be surprisingly easy to conduct against a large organization, where one does not personally know everyone in the organization.

<sup>21</sup> For example, the production of energy – as well as the ability to attack an energy plant – can require a knowledge of systems and computer languages that is truly unique to that environment.

dology for Water (RAM-W), which could then be used for self-assessment (Preimesberger, 2006).

Today, an important trend in CDXs is to encompass international partners. Because the architecture of the Internet is international in scope, Internet security is by definition an international responsibility.

In 2006, the U.S. Department of Homeland Security (DHS) began a bi-annual, international CDX called Cyber Storm. This event specifically seeks to assess how well government agencies and the private sector can work together to thwart a cyber attack.<sup>22</sup> The 2006 scenario simulated an attack by non-state, politically-motivated “hacktivists” (Chan, 2006). The 2008 Cyber Storm II<sup>23</sup> simulated a nation-state actor that conducted both cyber and physical attacks on communications, chemical, railroad, and pipeline infrastructure.<sup>24</sup> In 2010, Cyber Storm III added the compromise of trusted Internet transactions and relationships, and included cyber attacks that led to the loss of life.

The testing of cyber defenses is not confined to the First World. In 2009, the U.S. sponsored an international CDX in remote and mountainous Tajikistan, which included participants from Kazakhstan, Kyrgyzstan and Afghanistan (BBC, 2009).

## 5. Baltic Cyber Shield

Baltic Cyber Shield (BCS), held on 10-11 May 2010 in numerous countries across northern Europe, was a “live-fire” CDX. A twenty-person international RT and six national BTs took part in an unscripted battle in which the use of malicious code – within the confines of a virtual battlefield<sup>25</sup> – was both authorized and encouraged.

BCS 2010 was similar in nature to the annual CDXs that pit U.S. military services against one another (Caterinicchia, 2003), and for which the Pentagon now sponsors a national competition at the high school level.<sup>26</sup> Other CDXs that

<sup>22</sup> Market forces, deregulation, and outsourcing mean that myriad important computer networks and critical infrastructures now lie in private hands (Verton, 2003). This, combined with the reluctance of many businesses to disclose cyber attacks for fear of embarrassment, make it difficult for government to help protect the private sector.

<sup>23</sup> This CDX included eighteen federal agencies, nine U.S. states, three dozen private companies, and four foreign governments: Australia, Canada, New Zealand, and the UK. These were the same countries that took part in 2006; it is worth noting that these governments are members of a joint 1947 intelligence-sharing accord which makes it possible for them to share classified information.

<sup>24</sup> The RT also targeted the media in an effort to undermine public trust in government (Waterman, 2008).

<sup>25</sup> The entire CDX took place within the bounds of a safe, laboratory environment.

<sup>26</sup> In March 2010, “Team Doolittle” from Clearfield High School in Utah won the CyberPatriot II Championships, sponsored by the U.S. Air Force Air Warfare Symposium in Orlando, Florida. (*Defense & Aerospace*, 2010)

inspired aspects of BCS 2010 included the Pentagon's International Cyber Defense Workshop (ICDW), the UCSB International Capture the Flag (iCTF) and the U.S. National Collegiate Cyber Defense Competition.

The game scenario described a volatile geopolitical environment in which a hired-gun, Rapid Response Team of network security personnel defended the computer networks of a power supply company against increasingly sophisticated cyber attacks sponsored by a non-state, terrorist group.<sup>27</sup>

BCS 2010 had three primary goals. First, the BTs should receive hands-on experience in defending computer networks containing Critical Information Infrastructure (CII) and elements of Supervisory Command and Data Acquisition (SCADA).<sup>28</sup> Second, the CDX scenario sought to highlight the international nature of cyberspace, to include the political, institutional, and legal obstacles to improved cyber defense cooperation. Third, participating teams were meant to gain a better understanding of how to conduct CDXs in the future.

The WT was based primarily at SNDC in Stockholm, Sweden, with a smaller contingent at CCD CoE in Tallinn, Estonia. The WT's scoring criteria were designed to gauge the BTs' ability to maintain the CIA of their virtual networks, including office infrastructure and external services.<sup>29</sup> In the event of compromise, the number of points lost depended on the criticality of the system, service, or penetration. For example, if the RT gained Admin/Root-level access to a computer or compromised a SCADA Programmable Logic Controller (PLC), the BT was significantly penalized. On the other hand, BTs won positive points for thwarted attacks, for successfully completing in-game "business requests,"<sup>30</sup> and for the implementation of innovative cyber defense strategies and tactics.

The six BTs consisted of 6-10 personnel each, and hailed from various northern European government, military, private sector and academic institutions. All were provided an identical, pre-built, and somewhat insecure computer network composed of 20 physical PC servers running a total of 28 virtual ma-

---

<sup>27</sup> James Lewis of CSIS recently stated: "It remains intriguing and suggestive that [terrorists] have not launched a cyber attack. This may reflect a lack of capability, a decision that cyber weapons do not produce the violent results terrorists crave, or a preoccupation with other activities. Eventually terrorists will use cyber attacks, as they become easier to launch..." (Lewis, 2010).

<sup>28</sup> SCADA systems can be used to support the management of national critical infrastructures such as the provision of electricity, water, natural gas and manufacturing. The disruption or other misuse of such systems could potentially become a national security issue.

<sup>29</sup> Both automated and manual means were used to verify CIA. The latter, for example, could entail the WT simulating the actions of ordinary users. They may periodically request a BT webpage to see that it is reachable and not defaced.

<sup>30</sup> This aspect of the game was intended to raise the stress level of BT participants. It simulated the real-world challenge of handling both security threats and ordinary business processes at the same time. For example, a CEO may call while on a business trip, needing immediate, remote access and the BT must provide a timely solution. Alternatively, a BT member might become "ill" and have to spend one hour on "sick leave" in a break room.

chines.<sup>31</sup> These were further divided into four VLAN segments – DMZ, INTERNAL, HMI,<sup>32</sup> and PLC. The BT networks were further connected to various in-game servers that provided additional business functionality to their fictitious users.

The BCS 2010 scenario called for the inclusion of SCADA software in order to simulate a power generation company's production, management and distribution capabilities. These comprised GE PLCs, Simplicity HMI terminals, Historian databases, and two physically-separated model factories per BT network.

Because of the “rapid response” nature of the BCS 2010 scenario, the BTs were given access to the CDX environment – including somewhat outdated network documentation – only on day one of the CDX. They were allowed to harden their networks,<sup>33</sup> but a minimum number and type of applications and services had to be maintained.<sup>34</sup> The BTs were allowed to install new software and/or modify existing software. However, offensive BT cyber attacks, either against the RT or against other BTs, were strictly prohibited.<sup>35</sup>

The BCS RT consisted of twenty volunteers<sup>36</sup> from throughout northern Europe.<sup>37</sup> The RT was given access to the game environment two weeks' prior to the CDX in order to simulate a degree of prior reconnaissance. To maximize the CDX's value to all participants, the WT directed the RT to begin its attacks slowly, and to progressively increase the scale and sophistication of its attacks throughout the game. Beyond that, there was no limit on the type of hacker tools and techniques that the RT could use.<sup>38</sup> The RT was strictly prohibited, however, from attacking the CDX infrastructure,<sup>39</sup> and all attacks were confined to the virtual game environment. Internally, the RT divided itself into four sub-teams, de-

---

<sup>31</sup> The BTs accessed the game environment by VMWare Console from a browser or over SMB, RPC, SSH, VNC, or RDP. The power company's network included both Windows and Linux operating systems. Unfortunately, the Console access of the free version of VMWare Server proved to be too slow and unstable for such a large event.

<sup>32</sup> Human Machine Interface: these workstations ran the control software for the PLCs, providing the communication link between the Supervisor node and the remote factories.

<sup>33</sup> In the real world too, new IT hires cannot assume that legacy systems are secure or even properly installed. They are likely to find some vulnerable, unpatched, redundant, etc systems. Further, existing documentation may be dated or incomplete. Once given access to the infrastructure, the BTs were allowed to disable, patch and/or replace applications and services as long as the final configuration met CDX parameters.

<sup>34</sup> These included HTTP, HTTPS, SMTP, DNS, FTP, IMAP/POP3, SSH, and NTP.

<sup>35</sup> As a starting point, the BTs must stay within their countries' legal frameworks.

<sup>36</sup> The BCS 2010 RT was mostly volunteer-based. However, it is worth noting that one contractor bid to provide an RT came in at \$500,000.

<sup>37</sup> The Estonian Cyber Defence League built and managed the RT.

<sup>38</sup> However, it is helpful if many easily-accessible, Internet-available attack tools are used, because the BTs will see these often in the real world.

<sup>39</sup> Including the game scoring system ☺.

pending on the hackers' attack specialization: "client-side", "fuzzing", "web app", and "remote".

The GT, based at the Swedish Defence Research Agency (FOI) in Linköping, Sweden, hosted most of the BCS 2010 infrastructure. The BT networks were designed collaboratively by the GT and the WT. The FOI laboratory consisted of nine racks, with twenty physical servers in each rack.<sup>40</sup> The game infrastructure included twelve, twenty-centimeter-tall physical models of factories, each with its own PLC, SCADA software, and "Ice Fountain" fireworks that the RT could turn on as "proof" of a successful attack. The GT provided the RT and BTs access to the game environment via OpenVPN.

Finally, the WT had access to a robust visualization environment<sup>41</sup> that displayed all network topography, network traffic flows, observer reports, chat channels, team workspaces, scoreboard, and a terrestrial map of the CDX environment.<sup>42</sup>

## 6. BCS execution

BCS 2010 formally began when the BTs and the RT logged into the CDX environment. But the most anticipated moment arrived when the RT began its cyber attack on the BT networks.

The RT campaign was divided into four phases:

1. Declaration of war
2. Breaching the castle wall
3. Owning the infrastructure
4. Wanton destruction

The first objective, declaration of war, required the RT to "deface" the six BT public websites, and to give each power company an ultimatum. In a posted statement, the "cyber warfare division" of an extremist environmental organization called "K3" demanded that the power company publicly announce its intention to convert to alternative, greener power ... or face a crippling cyber attack. The RT succeeded in defacing five of the six sites within 30 minutes.

---

<sup>40</sup> The servers had 2 Xeon 2.2 GHz processors, 2 GB RAM, 80 GB HDD, VMware Server 2.0.2 on Gentoo Linux, 2x Ethernet interfaces, and 2 switches, one for management and one for the game network.

<sup>41</sup> This was provided by the Finnish company Clarified Networks.

<sup>42</sup> In the BCS 2010 scenario, two BTs were theoretically based in South America, two in Africa and two in Asia; the RT was in Iceland (in reality, all teams were located in northern European countries).

During phase one, the RT was allowed to compromise only one server in each BT DMZ and only one internal workstation in each BT network. Even with these constraints, however, the RT succeeded in creating such a steady stream of incident reports that the WT had trouble translating all of them into negative points for the BTs. For example, within an hour the RT had established a live audio and video connection into one BT network; in other words, the game had barely begun and a digital spy was already working inside one of the power companies.

In the past, a major challenge inherent in CDXs is that it has been difficult for the RT to maintain balanced and sustained pressure on all BTs throughout the game. At different stages in a CDX, some BTs could be quite busy while others had nothing to do. To help avoid this, the WT instructed the RT that, for each vulnerability discovered on a BT network, the RT must systematically check all other BT systems for the same vulnerability and exploit it if possible.

Phase two of the K3 attack campaign called for the RT to compromise as many DMZ<sup>43</sup> systems as possible. At the end of day one, the RT had successfully attacked 42 computers, including web and email servers. The RT leader was more than pleased with his team's progress.

Phase three called for the RT to steal the BT networks' "crown jewels." In BCS 2010, these were the internal network computers that served as the HMI for power generation and management, i.e. its SCADA infrastructure. Although the RT was quite successful in the CDX overall, it claimed only limited victories in phase three. Of the twelve model factories, the RT succeeded in setting only one of them on fire, and it is still unclear whether this RT success was intentional or accidental.<sup>44</sup>

The fourth and final phase of BCS 2010, "wanton destruction," allowed the RT to attack and destroy any BT system in the CDX. The goal was to simulate a desperate attempt by K3 to cause maximum disruption to the power companies' operations. Unfortunately, RT successes in this phase often denied service to the same computers it had previously compromised, and it prevented the WT from scoring the game properly. In other words, a poorly-designed DoS attack can bring down large sections of network infrastructure and nearly ruin the game. In this CDX, for example, the RT used a custom-configured Cisco router to simulate traffic; at one point, it created such a high volume of data that the RT denied itself access to the gamenet for 15 minutes.

The RT successfully attacked several publicly-known vulnerabilities during BCS 2010, including MS03-026, MS08-067, MS10-025, and flaws in VNC,

---

<sup>43</sup> The DMZ, or demilitarized zone, is a physical or logical subnetwork that is exposed to untrusted networks, such as the Internet.

<sup>44</sup> The RT may have gotten lucky while examining the SCADA Modbus protocol with their fuzzing tools.

Icecast, ClamAV, and SQUID3. It hacked web applications such as Joomla and Wordpress, and employed SQL injection, local and remote file inclusion, path traversal, and cross-site scripting against Linux, Apache, Mysql, and PHP. Other tactics included account cracking, online brute-forcing, DoS with fuzzing tools, obtaining password hashdumps of compromised systems and using the “pass-the-hash” technique to hack into more machines. The RT installed Poison Ivy, netcat and custom made code as backdoors. Metasploit was used to deploy reverse backdoors. The RT modified compromised systems in various ways, such as altering the victim’s crontab file to continuously drop firewall rules. Last but not least, the RT possessed a zero-day client-side exploit for virtually every browser in existence today.

Although the BCS 2010 scoring system applied only to the BTs, when the game was over the RT leader smiled as if his team had won the game. When the CDX ended, there were over 80 BT computers that were confirmed compromised.

However, the BTs did adopt some successful defensive strategies. The most successful BT – which was also declared the winner of BCS 2010 – quickly moved essential network services, such as NTP, DNS, SMTP and WebMail, to its own, custom-built, higher-security virtual machine. IPsec filtering rules were used for communications with the Domain Controller. This BT had also requested the use of an “out-of-band” communication channel for its discussions with the WT, i.e. not the in-game e-mail system, which it assumed might be compromised. Finally, the winning BT was successful in finding and disabling preexisting GT-installed malware.<sup>45</sup>

BCS 2010 also highlighted the value of numerous current OS-hardening tools and techniques. For Linux computers, these included AppArmor, Samhain, and custom short shell scripts; for Windows, Active Directory (AD) group policies, the CIS SE46 Computer Integrity System, Kernel Guard, and the central collection of event logs. For all OSs, the white/black-listing and blocking/black hole-routing of offending IP addresses, on a case-by-case basis, proved invaluable.

## 7. Conclusion

The Cooperative Cyber Defence Centre of Excellence (CCD CoE), the Swedish National Defence College (SNDC) and the Swedish Defence Research Agency (FOI) believe that BCS 2010 accomplished its three primary goals.

First, the GT network infrastructure provided a sufficiently robust environment for a rare “live fire” CDX that offered six professional BTs the opportunity to defend CII and SCADA-enabled computer networks against a highly-motivated, capable RT. All teams were fully occupied throughout the two-day

---

<sup>45</sup> Preexisting malware can simulate what a Rapid Response Team would likely find on any computer network.

exercise, and very little down-time was reported. Further, the BCS 2010 scenario described a “cyber terrorist” threat that may already endanger the national security of governments around the world (White House, 2009; CBS, 2009).

Second, BCS 2010 was a truly international exercise. Because cyber attacks can be launched from anywhere in the world, and are likely to traverse third-party countries en route to a target, it is critical to develop cross-border relationships before an international crisis occurs. In BCS 2010, over 100 personnel from seven countries participated. Numerous international partnerships were either established or strengthened during the course of this project.

Third, BCS 2010 conducted a post-exercise participant survey with a view toward providing a list of lessons learned to future CDXs around the world.<sup>46</sup> Here are the highlights:

- There should be at least one WT member per BT and two WT members on the RT to allow for sufficient observation, communication, adjudication, and clarification on scoring.
- The WT should include a cyber-savvy lawyer to shed light on the legality of unscripted attack and defense scenarios.
- Each BT must have at least one full-time WT-appointed “dumb user” active on the virtual network to make client-side attacks possible.<sup>47</sup> In BCS 2010, the RT did not have the chance to use a powerful “zero-day” browser exploit with which they had intended to target the virtual power company employees.
- Prior to a “live-fire” CDX, all participants should devote one full day to testing connectivity, bandwidth, passwords, cryptographic keys, etc., and for clarification on rules and scoring.
- The VMWare Server Console was too slow for the high demands BCS 2010 placed upon it, and it cannot be recommended to other CDXs.
- The WT/GT should grant the BTs some network administration rights over their physical machines in the CDX environment. Otherwise, installing and patching software can be too time-consuming.
- A “wanton destruction” phase (i.e. one without a clearly defined purpose and certain limits on the RT) will likely destroy the game itself, and so for most CDX scenarios cannot be recommended.
- In a project this big, some egos and agendas are bound to clash. It is important to designate diplomatic yet authoritative personalities, who can meet team-oriented deadlines, from the beginning.

---

<sup>46</sup> The author gave a BCS 2010 presentation at DEF CON 18: [www.defcon.org/html/links/dc-archives/dc-18-archive.html#Geers](http://www.defcon.org/html/links/dc-archives/dc-18-archive.html#Geers).

<sup>47</sup> This cannot be an integral BT member due to the obvious conflict of interest.

Finally, one of the lessons of BCS 2010 is that many of the challenges inherent in conducting a robust CDX mirror the challenges of managing both IT and cyber security in the real world. Cyberspace is complicated, polymorphic, dynamic, and evolving. Cyber defenders may never see the same attack twice. The intangible nature of cyberspace can make even the calculation of victory, defeat, and battle damage a highly subjective undertaking. And believe it or not, even knowing *whether* one is under cyber attack can be a challenge.

## References

- Adams, J. (2001). "Virtual Defense," *Foreign Affairs* 80(3) 98-112.
- "Air Force Association; Utah's Team Doolittle Wins CyberPatriot II in Orlando." (2010, Mar 10). *Defense & Aerospace Business*, p. 42.
- Bliss, J. (2010, Feb 23) "U.S. Unprepared for 'Cyber War', Former Top Spy Official Says," *Bloomberg Businessweek*, online.
- Caterinicchia, D. (2003, May 12) "Air Force wins cyber exercise." *Federal Computer Week*, 17(14), p. 37.
- Chan, W. H. (2006, Sep 25). "Cyber exercise shows lack of interagency coordination." *Federal Computer Week*, 20(33) p. 61.
- "Cyber War: Sabotaging the System." (2009, Nov 8). *60 Minutes: CBS*.
- Geers K. (2010). "The challenge of cyber attack deterrence." *Computer Law and Security Review* 26(2) pp. 298-303.
- Geers, K. (2008, Aug 27). "Cyberspace and the Changing Nature of Warfare." *SC Magazine*.
- Gibbs, W. W. (2000). "RT versus the Agents." *Scientific American*, 283(6).
- Goble P. (1999, Oct 9). "Russia: analysis from Washington: a real battle on the virtual front." *Radio Free Europe/Radio Liberty*.
- Gomes, L. (2003, Mar 31). "How high-tech games can fail to simulate what happens in war." *Wall Street Journal*.
- Gorman, S. (2009, Aug 17) "Cyber Attacks on Georgia Used Facebook, Twitter, Stolen IDs." *Wall Street Journal*.
- "International cyber exercise takes place in Tajikistan." (2009, Aug 6). *BBC Monitoring Central Asia*. (Avesta website, Dushanbe)
- Keizer, G. (2009, Jan 28). "Russian 'cyber militia' knocks Kyrgyzstan offline." *Computerworld*.
- Lam, F., Beekey, M., & Cayo, K. (2003). "Can you hack it?" *Security Management*, 47(2), p. 83.
- Lawlor, M. (2004). "Information Systems See Red." *Signal* 58(6), p. 47.
- Lewis, J.A. (2010) "The Cyber War Has Not Begun." *Center for Strategic and International Studies*.

- Meserve, J. (2007, Sep 26). "Sources: Staged cyber attack reveals vulnerability in power grid." *CNN*.
- Orr, R. (2007, Aug 2). "Computer voting machines on trial." *Knight Ridder Tribune Business News*.
- Preimesberger, C. "Plugging Holes." (2006). *eWeek*, 23(35), p. 22.
- "Remarks by the President on Securing our Nation's Cyber Infrastructure." (2009). *The White House: Office of the Press Secretary*.
- "Tracking GhostNet: Investigating a Cyber Espionage Network." (2009). *Information Warfare Monitor*.
- Verton, D. (2003) "Black ice." *Computerworld*, 37(32), p. 35.
- Verton, D. (2002). *The Hacker Diaries: Confessions of Teenage Hackers*. New York: McGraw-Hill/Osborne.
- Wagner, D. (2010, May 9). "White House sees no cyber attack on Wall Street." *Associated Press*.
- Waterman, S. (2008, Mar 10). "DHS stages cyberwar exercise." *UPI*.
- "'USA Today' Website Hacked; Pranksters Mock Bush, Christianity." (2002, JUL 11). *Drudge Report*.