An Overview of Cyber Attack and Computer Network Operations Simulation

Sylvain P. Leblanc,
Andrew Partington
Computer Security Laboratory
Royal Military College of Canada
Sylvain.Leblanc@rmc.ca

Ian Chapman,
Mélanie Bernier
Centre for Operational Research and Analysis
Defence Research and Development Canada
Ian.Chapman@drdc-rddc.gc.ca
Melanie.Bernier@drdc-rddc.gc.ca

Keywords: Overview, Survey Paper, Cyber Attacks, Cyber Warfare, Computer Network Operations

Abstract

This paper represents a snapshot of the current state of the art in the simulation and modeling of cyber attacks and defensive responses to those. It discusses a number of simulations of cyber warfare, including live, virtual, and constructive simulations. The simulations discussed in this paper were found in the open literature and were conducted in the private sector, academia, and government. Each simulation is briefly described, including goals, methodology, and a brief discussion of its accomplishments. These modeling and simulation efforts are of particular interest to the military modeling and simulation community, as it is likely that military forces will continue to rely ever more heavily on computer and communication networks.

1. INTRODUCTION

The concepts and technical challenges behind the simulation of military conflicts in the traditional operational domains – land, maritime, and air – have been well understood for several decades, and thus numerous applications have been developed to support computer wargaming. These wargames are typically used to support training and experimentation, and are seen as a safe and cost-effective way to assess the effects of new technologies and equipment before deploying them to the real battlefield.

Recent events, such as the 2007 cyber attack on Estonia, have shown the rising importance of computer network operations (CNO)[1] in an increasingly inter-networked world. Both civilian and military domains have become increasingly reliant on computer networks for communication, information management, utilities management, financial systems, air traffic control, and many other critical applications. In fact, the authors argue elsewhere at this conference that CNO education is vital for both technical and non-technical commanders, and propose using simulation to further these educational goals [1].

[1] Per US Doctrine, CNO is comprised of Computer Network Defense (CND), Computer Network Attack (CNA) and Computer Network Exploitation (CNE). Many sources use cyber warfare; we use both terms.

Cyber attacks have the potential to be extremely disruptive to a wired society. To understand some of the ramifications of these events, including their potential impact on the use of networks, the research community has begun the development of a number of applications to simulate cyber warfare.

The paper is separated in two main sections. The first part will discuss prominent private sector and academic research, while the second will discuss public sector research in the field of modeling and simulation for cyber warfare.

This paper is intended to present the results of our survey of current unclassified research literature, openly published on the topic of simulation for cyber warfare. It is not meant to be all encompassing. The authors have not found other works that attempt to summarize key efforts in this area of study.

The authors believe that simulation will make ever greater contributions to the field of cyber warfare and CNO. This paper and the Military Modeling Symposium that flow from it should be viewed as an attempt to engage the research community on this important emerging topic.

2. PROMINENT PRIVATE SECTOR AND ACADEMIC RESEARCH

The idea of simulating cyber attacks has been investigated by several researchers and students at universities as well as in private organizations. The simulations discussed in this section have been selected for discussion because they represent some of the most significant work in cyber attack modeling.

2.1. Cyber Attack Modeling using ARENA

ARENA is a constructive simulation developed by researchers at the Rochester Institute of Technology (RIT), partially sponsored by the U.S Air Force Research Laboratory (AFRL) in Rome, NY. The ARENA simulation software was used to simulate cyber attacks against a computer network from an external source such as the internet [2-3].

The simulation models step-by-step attacks on a computer network. The attacks can be automatically created within the constructs of the tool, or they can be predefined in XML files that can be loaded by the simulation tool. Each

attack has a specific associated attack type and a target computer on the network under attack. The simulation supports a variety of attack types such as Denial of Service (DoS) attacks and the installation of a backdoor on a target computer. Each attack will typically go through numerous steps to attempt access to a target computer. Therefore, each attack will typically involve an attacker infiltrating several intermediary computers and servers on a network in order to compromise the target computer. Along with its defined type and target, each attack includes characteristics of the attacker by giving a normalized value for efficiency, stealth and skill. Efficiency refers to the speed and swiftness with which the attacker can move from one intermediary host to another in a multi-tiered network. Stealth refers to the attacker's ability to avoid unnecessary intermediate steps which may alert network defenders to his presence. Finally, the attacker's skill parameter is used to determine stochastically the success of each intermediary steps required to prosecute the attack against the target computer.

The ARENA simulation also allows the user to construct a computer network and execute a series of cyber attacks on target hosts within that network. The simulated network can be multi-tiered, with several layers separated by routers and other network hardware. Host characteristics can be specified such as the IP address, the operating system, and the type of Intrusion Detection System (IDS) sensor used on the hosts (servers or client computers). Once the network is created, attacks can be simulated manually (by choosing the attack type, the target and the time when the attack is launched) or automatically (by using pre-defined XML attack files). Statistics on the attacks can be collected by applying the attack details and attacker characteristics (the attacker's skill, stealth and efficiency parameters) against the target network architecture.

This ARENA simulation tool is primarily used to analyze IDS sensors. IDS sensors are deployed at specific locations within the target network to examine network traffic and generate alerts based on programmed rules. Not all alerts are legitimate; some are the result of attacks, while others are the result of non-malicious activity. The simulation outputs an attack log, detailing the target and the time of occurrence of each attack. The simulation also lists which attacks triggered alerts, and for each IDS, notes the details between the true and false positives.

Overall, this is a very well developed simulation tool capable of simulating many forms of attack on a specific, user-defined network. The focus on analysis of IDS sensors makes the output of the simulation somewhat limited, but useful nonetheless. At the end of a simulation run, the user is presented with a list of attacks that occurred on the simulated network and a list of the alerts reported by the IDS sensors. This output can help analyze the target network topology; however it offers limited benefits in training and experimentation.

2.2. RINSE

The Real-Time Immersive Network Simulation Environment (RINSE) is a live simulation developed by researchers at the University of Illinois at Urbana-Champaign in 2006 [4]. RINSE was designed with the aim of developing a simulation capable of supporting large-scale wide-area networks (WAN) consisting of hundreds of local-area networks (LAN), each administered by users. In RINSE simulations, attacks are carried out against the WAN and users attempt to diagnose and counter the attacks to keep their LAN's network services running.

Physically, the simulator consists of an enclosed network with several users acting as LAN managers on different computers joining the same simulation exercise. The users are tasked with the defence of their LAN against computer attacks carried out by the simulation tool. A game manager coordinates the simulation and plays the role of the attacker.

Through the command prompt, the user can input commands that fall into five different categories: attack, defence (such as the installation of packet filters), diagnostic networking tools (such as ping), device control (shutting down or rebooting devices such as hosts and routers), and simulator data.

The focus of the simulation is on external attack vectors such as Distributed DoS (DDoS), worms and other attacks involving high-intensity traffic flows. Simulator commands are used to control the output of the simulation in order to highlight the trace flow from a selected host.

RINSE also contains other useful features such as save points and the ability to vary the pace of the simulation. In addition, RINSE allows the game manager to adjust the resources of simulated computers, such as memory and CPU speed, which is important when modeling DDoS attacks.

In summary, RINSE is a very powerful and well designed live simulation tool capable of simulating attacks on complex networks involving a large number of network defenders. It is limited by the small number of cyber attacks that it can simulate. Also, the use of a command-line interface, instead of a full graphic user interface (GUI), makes its use cumbersome. While the tool helps with the training and education of network defenders, it does not contribute to the general understanding of the implications of CNO by senior leaders.

2.3. Simulating Cyber Attacks, Defenses and Consequences by Cohen

Simulating Cyber Attacks, Defences and Consequences is a paper written by Fred Cohen of Sandia National Laboratories in the year 1999 [5]. Despite its publication more than 10 years ago, the paper's discussion of developments in cyber attack simulation are still largely

relevant and have helped contribute to the work on Secusim (Section 2.4). Cohen's simulation is constructive, runs on a single computer and models various attacks on a simulated network.

Cohen simulates various attack scenarios using the attacker's and defender's skills as the primary simulation parameter. Cohen went to great lengths to classify attackers and gives them various attributes and skill levels. Each attack was given a classification such as vandalism, professional-theft, military or insider action. Combining these parameters and attributes yields 34 different classes of attackers. Each class has a different skill level, different predetermined attack goals and indication of their ability to hack stealthily.

This extensive classification scheme makes the simulation easier to understand and the results easily analyzed for different types of computer attackers. Unfortunately Cohen does not detail how he carried out the classifications. Even if he made very good generalizations about certain types of attackers, the differences between individuals are not captured by the simulation. Nevertheless the idea is intuitive and represents an interesting concept in cyber attack simulations.

Interestingly, Cohen's simulation is based on a set of 37 types of threats, 94 types of attacks, and approximately 140 types of protective methods. A database tracks the attacks and their associated protective methods. This was seen as very innovative as there is a variety of possible cyber attacks and only certain defences are possible against certain attacks. We see no evidence of validation of this extensive classification scheme.

The output of interest in the simulation is the simulated duration of the attack and its outcome (whether the attacker or the defender "wins"). The attacker will win if he achieves his goals and the defender will win if he successfully prevents the attacker from achieving his goals. Depending on the attacker's goals and the respective skill level of the attacker and defender, the simulated time of the attack can range from minutes to years. This is comparable to real life where attackers may try to accomplish their goals quickly or wait months or even years for the opportunity to attack.

Cohen extends the usefulness of his simulation by attempting to value the cost to the attacker and defender in terms of time spent and the expense of equipment used, focusing on the cost of a skilled defender versus an unskilled defender. He posits that hiring a very skilled computer administrator may be more expensive than the loss incurred from a cyber attack. Cohen's work in the modeling of cost is very simplistic; nevertheless considering the financial costs in a cyber simulation model is an idea that may have considerable appeal.

Cohen's simulation was ground breaking in scope, attempting to cover many forms of cyber attack and defence. However, Cohen admits a struggle with validating his model as he was unable to compare his simulation with large amounts of data from real world cyber attacks. However, he maintains that his simulation was validated by various experts who agreed that his model was accurate. Nevertheless, since it has been over 10 years since Cohen designed his simulation, and as he was unable to do much in the way of validation, one cannot place much faith in the accuracy of his model. Nevertheless, the ideas, concepts and methodology in his attempt to simulate cyber attacks are all very important and applicable to any modern simulation of cyber attacks.

2.4. SECUSIM

Secusim is constructive simulation software that was developed at the Department of Computer Engineering at Hangkong University in Korea in 2001 [6]. It was designed for the purpose of "specifying attack mechanisms, verifying defence mechanisms, and evaluating their consequences." It is programmed in C++ for use on a single computer and includes a GUI allowing the user to create a virtual computer network of his or her design.

The software has different modes: Basic, Intermediate, Advanced, Professional and Application. Each mode has different levels of functionality and customizability. The research paper contrasts the modes as follows:

- "Basic Mode: Provides basic knowledge of cyber-attack mechanisms by retrieving the scenario database.
- Intermediate Mode: Allows the cyber attack simulation of a given network by selecting arbitrary attacker model and target host as well as setting the attack scenario.
- Advanced Mode: Supports direct command-level testing of a given cyber-attack into the given network models.
- Professional Mode: Provides advanced analysis for link and node vulnerability of given network by allowing multiple cyber-attack simulation.
- Application Mode: Includes graphic editing capabilities allowing users to create and simulate their own customized network configurations."

The different modes enable users without much CNO expertise to operate the software in order to run the simulation while giving those with more knowledge the ability to design their own networks and test them against multiple cyber attacks in a single simulation run.

Secusim is interesting primarily because of its customizability and its user-friendly GUI. It builds on the initial research of Fred Cohen and provides a good example of simulation software used for cyber attack modeling and analysis.

2.5. Research Efforts Involving OPNET

There have been a few cyber attack simulations that use the computer software OPNET Modeler. This commercial simulation software is designed to aid in the analysis and

design of communication networks, devices, protocols, and applications. The software allows the modeling of "all network types and technologies" [7]. This includes VoIP, TCP, OSPFv3, MPLS, and IPv6. Among OPNET's many features are a user interface, support for simulations distributed across several computers and a library of device models with source code.

OPNET's ability to simulate computer networks makes it an ideal basis for a cyber attack simulation [7]. In this section, two research papers discuss the use of OPNET in cyber attack simulations.

2.5.1. Sakhardande - SUNY

"The use of modeling and simulation to examine network performance under Denial of Service attacks" is a master's thesis written by Rahul R. Sakhardande of the State University of New York in 2008 [8]. Sakhardande modeled a computer network in OPNET and analyzed its performance under normal operating conditions and again when undergoing a simulated DoS attack. The model was fairly limited as the authors did not configure OPNET to represent many different network topologies in order to conduct a more thorough analysis. Furthermore, Sakhardande was unable to properly validate his model against real operating environments. Nevertheless, the work shows that a model of DoS attacks on a network can be simulated using OPNET, even if the results in this particular instance were of limited general applicability.

2.5.2. Frequency-Based IDS

"A Frequency-Based Approach to Intrusion Detection" is a research paper written by Mian Zhou and Sheau-Dong Lang of the University of Central Florida in 2003 [9]. The simulation that they created using OPNET was primarily used to test an experimental intrusion detection algorithm. They tested the effectiveness of the detection algorithm by observing network intrusion data in a simulated network using OPNET while simulating several types of DoS attacks and probe attacks.

The two papers discussed above demonstrate that OPNET can be used to simulate a computer network sufficiently well for experimentation. However, OPNET modeling efforts reported in the literature were not detailed enough to assist in the training of network defenders or the education of senior leaders.

2.6. NetENGINE

The Institute of Security Technology Studies at Dartmouth College developed a cyber attack simulation tool called NetEngine in a paper published in 2003 [10]. The tool was designed to be a virtual simulation, involving several users on different computers connected to the same simulation program. NetEngine is designed to be able to represent very large IP networks and is intended to be used to train IT staff in combating cyber attacks.

NetEngine features a user interface where the user views network topology maps, the simulated network's status, and router load plots. The software is built so that it can be accessed through the web using an internet browser. The simulation software itself is written in C++ and is designed to be run on Linux machines. The simulation can model workstations, routers, firewalls, servers, host clusters and ISPs. Each user of the simulation is placed in charge of a simulated domain which is a collection of hardware and software systems on the simulated computer network. Various cyber attacks are launched against these simulated domains. The users are able to communicate with each other during the simulation by using simulated email, facsimile, telephone or instant message. These communications processes are also vulnerable to the simulated cyber attacks. This allows team work to play a role in the simulation.

This simulation tool does not focus on the technical details of the attacks but instead focuses on their effects. Therefore, the simulation implements generic attacks such as DDoS attacks, viruses and worms but makes little attempt to simulate attacks that rely on targeted computer exploits. The simulated attacks are predetermined and released according to a master driving script. This script effects state changes in the network to simulate an attack. For example, it can change the load level on a particular link or change the status of routers, workstations and other devices to simulate compromises or service degradation. Although the master driving script contains details and release time for each attack, these are first reviewed by an exercise controller who can either accept or cancel the release of the scripted attack.

NetEngine has been quite successful. It was used as the basis of Livewire, a four day US national cyber defence exercise conducted in October 2003. This exercise involved over 300 participants in the US, including representatives from the energy and finance sectors. The exercise simulated a cyber attack against critical infrastructures which required the participants to communicate and work together to defend against the attacks or mitigate their impact. NetEngine has proven to be very useful simulation software with the ability to simulate large computer networks under cyber attacks.

2.7. Concluding Remarks on Prominent Private Sector and Academic Research Efforts

The private sector and academia have conducted substantial research on cyber attack modeling. Many of the simulations have been constructive simulations, automated to execute without much user intervention [2,5,6,8,9]. These provided results that enabled the discovery of general patterns in cyber attacks but the accuracy of these results are dependent on the models used to drive the simulation.

Unfortunately most of these models offer little in the way of validation, a fact well captured by Fred Cohen who states that it is very difficult to set parameter values and adjust simulation mechanisms within a cyber attack simulation that are validated against real world events. Similarly, the virtual and live simulations discussed in this section may also suffer these same problems because of poorly defined attack scenarios [1,4,7,10,11]. It appears that live simulations are more geared towards education than analysis of computer attacks in general, and as such, non-validated attack details still allow the simulations to be effective educational tools.

It is worth noting that the constructive simulations and virtual simulations discussed above focused on the effects of attacks on computer networks while mostly ignoring the bigger effect they can have on an organization or nation. If one wishes to understand these larger-scale effects (as was the case in many live simulation efforts), it stands to reason that the scope must be widened and the details of the attacks must be abstracted.

3. PUBLIC SECTOR RESEARCH

Governments throughout the world, along with their military forces, have become increasingly interested in the applications of CNO as well as the necessity to defend against domestic or foreign cyber attacks. By far, the largest CNO research presented in the open literature comes from the US, France, China and Israel. While recent events such as StuxNet and GhostNet suggest that Israel [12] and China [13] may have links to CNO, the open literature does not offer much insight into their efforts. Our discussion of public sector research will therefore not involve China or Israel.

By no means is the information presented here complete. The majority of CNO research, especially recent work, conducted by military forces is classified and thus inaccessible. In this section we discuss the information on simulations of cyber attacks that has been garnered from public sources, through such means as press releases and public reports, on the results of simulations. Unfortunately, this means that even though results are sometimes published, the specific simulation methods are not discussed in detail.

3.1. US Cyber Command and Air Force Cyber Operations Division

The US Cyber Command (USCYBERCOM) is subordinate to the US Strategic Command [14]. It acts as a sub-unified command with service elements from the US Army (Army Cyber Command), the US Air Force (24th US Air Force), the US Navy (Fleet Cyber Command/10th Fleet) and the US Marine Corps (Marine Forces Cyber Command).

USCYBERCOM was formed in May 2010, when it achieved initial operational capability. It achieved full operational capability, meaning that it demonstrated the ability to accomplish its mission, at the end of October 2010 [15]. Although a military audience would surely be able to contribute much more on CYBERCOM, we offer the following from information available in the open literature.

Its published mission statement reads: "USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."[14]

The service components listed above were in existence before CYBERCOM was established. CYBERCOM's status as a sub-unified command reflects a recognition by senior leadership that CNO affect numerous armed services, and that effective cyber responses required coordination and leadership. An interesting development in the evolution of CYBERCOM is the suggestion by some authors that because the traditional Army, Navy, Air Force and Marine cultures have difficulty dealing with CNO, a separate branch of service should be established for cyber operations [16].

Although one should expect much from USCYBERCOM in the future, recent US military cyber simulation efforts come mostly from the US Air Force.

The US Air Force modified its mission statement “to deliver sovereign options for the defense of the US of America and its global interests - to fly and fight in Air, Space, and Cyberspace” in 2005. The addition of the word “Cyberspace” has had a major impact on their subsequent outlook toward CNO. The US Air Force has been a leading innovator in cyber warfare [17]. Most recently, in June 2010, a new officer training course in cyber warfare has been developed with a budget of $US 11.7 million. This included $US 7.6m spent on upgrades of facilities, computer infrastructure, laboratory networks and “simulators” [18].

Even though the news article announcing this development did not specify what these simulators are, it is known that the US Air Force has been developing and experimenting with at least two simulation programs over recent years: SIMTEX and CAAJED.

3.1.1. SIMTEX

The Simulator Training Exercise Network (SIMTEX) is a simulation infrastructure used in training to automatically simulate various computer network attacks. The simulator mimics the three tier network architecture of the US Air Force. It can be set up to link together multiple simulators to form an “intra-network” [19].The simulator includes a simulated internet with domain name resolution complete with mimicked websites such as Google.com and CNN.com.

Bulwark Defender, whose previous incarnation was known as Black Demon, is a training exercise using the SIMTEX infrastructure. This training exercise is carried out once a year by military services and government agencies [20]. Participating services and agencies train against simulated cyber enemies that attempt to steal information and cause damage to their computer networks. Overall, SIMTEX is widely used and is therefore an important virtual simulation infrastructure.

3.1.2. CAAJED '06

While SIMTEX simulates the mechanics of an attack on a computer network, CAAJED focuses on the bigger picture and the kinetic effects of cyber attacks in a war situation [21]. CAAJED is a manual integration of CNO and cyber attacks with the US Air Force war simulator Modern Air Power (MAP). CAAJED consists of all the features of MAP such as the ability to play the war game as a human versus human, human versus computer opponent, or computer versus computer contest.

In CAAJED, the cyber attacks are not automatically controlled by computers but are manually implemented by operators. When the cyber attacks affect network services the operators are instructed to disable or degrade the associated assets. Assets (including air bases, SAM sites, radar sites, and individual aircraft) have capabilities (such as anti-aircraft artillery, radar coverage, ability to launch aircraft) which can be enabled, disabled or reduced in effectiveness through cyber attack. The users of the simulator were not aware that the operators sitting at consoles helped simulate the cyber attacks, but they were able to observe effects that were consistent with the simulated cyber attacks. Overall, while this simulation was implemented as a proof of concept, it showed a lot of potential as a method of more seamlessly integrating simulated cyber attacks in a wargame. The CAAJED simulation was used in a Cyber Defence Exercise in 2007. This took the form of a competition between two teams where each team only controlled the cyber warfare elements while a constructive simulator controlled the remaining MAP elements. The participating undergraduate teams were scored to make the exercise more interesting to the participants, but these scores were not analytical in nature; they were not considered valid analytical data..

Overall, the US Air Force's recent focus on cyber warfare has led them to produce useful simulations. There is a big difference between SIMTEX's simulation of CNOs at the network level and the bigger picture view that is provided by the CAAJED simulation. Regardless, both types of simulations are valuable, achieving very different training and simulation goals.

3.2. USMA IWAR and RMC CSL

The Information Warfare Analysis and Research (IWAR) laboratory at the US Military Academy (USMA – West Point, NY) is a network attack and defence simulator used to train cadets and faculty in information warfare [22]. It is capable of simulating defences such as cryptography, encryption and access control methods. IWAR is also able to simulate attacks such as Trojan horses, vulnerability scanners, viruses, worms, DoS, DDoS, and password hacking.

IWAR is more akin to a large isolated network than simulation software. It requires extensive effort to maintain and the set-up for each use is very complex. While in use, IWAR requires very close monitoring and its configuration must be adjusted to ensure that it can support the aims of the exercise for which it is being used.

The RMC Computer Security Laboratory (RMC CSL) uses a similar isolated network for CNO education and training, allowing us to gain perspective into the efforts required to run such a network. The RMC CSL isolated network uses virtualization software to enable multiple guests to run on a series of physical hosts. These virtual hosts can be configured to represent the hosts on a network, which can then be attacked and defended. The RMC CSL infrastructure requires a full time technician to maintain approximately seven physical hosts hosting approximately 15 – 20 guests being defended by approximately 10 – 15 participants. In addition, the RMC CSL isolated network typically employs an attack team of some five to eight members, and exercise coordination cell of approximately three to five controllers. Running such an isolated network is not cheap.

Notwithstanding the lack of automated simulation software and resource costs involved in their use, the IWAR and RMC CSL isolated network are very successful and they are continuously being evolved and improved upon. The IWAR and RMC CSL isolated networks have been used for the NSA sponsored annual Cyber Defence Exercise (CDX). The USMA has used IWAR since the inception of the CDX in 2000 and the RMC CSL has used its isolated network since 2009. The CDX is an annual competition for the US Military, Naval, Air Force, Merchant Marine, and Coast Guard Academies as well as the Air Force Institute of Technology, the Naval Postgraduate School and the Royal Military College of Canada. Each institution is tasked with the design and implementation of a network in support of a notional NATO operation. Each institution monitors its network through their network operation centre, and must respond to attacks being carried out by an NSA attack team.

3.3. Cyber Storm I, II and III

Cyber Storm I,II and Cyber Storm II were live simulations conducted in February 2006, March 2008 and September 2010 respectively [23-24]. The three simulation exercises were developed by the US Department of Homeland Security National Cyber Security Division. Cyber Storm involved over 100 participants from industry,

military and government, mostly from the US, but also including participants from the UK, Canada, Australia and New Zealand. Cyber Storm II was essentially a repetition of Cyber Storm I with more participants and different scenarios acted out. For its part, Cyber Storm III added yet more international, state and private sector participation. Cyber Strom III was also the first opportunity to exercise the National Cyber Incident Response Plan and helped test the National Cyber Security and Communications Integration Centre. As Cyber Storm I, II and III were very similar, they will be discussed at the same time.

The exercise had the aim of examining the "preparedness, response, coordination, and recovery mechanisms to a simulated cyber event within international, Federal, and State Governments in conjunction with the private sector" [23]. As a result, the simulation was mostly about education, bringing attention to the problem of international cyber security, and assessing how well different organizations from across the world can work together in the face of cyber attacks.

The simulation itself saw organizations receiving cyber attack injects related to several scenarios over the course of four days and requiring them to work with other organizations to develop strategies and responses to the attacks. The simulation was not designed to test the technical security of computer networks but instead to test the policy response of organizations and their ability to coordinate with other organizations. The various scenarios involved cyber attacks on infrastructure within the Energy, Information Technology, Transportation and Telecommunication sectors.

Even though Cyber Storm did not focus on the actual methodologies of cyber attacks and their prevention, it still had great value as it simulated the effects of cyber attacks and brought many organizations together to think about potential cyber threats and how they would respond to them. Highlighting the potential threat from cyber attacks, along with practicing cooperation across industries and the public sector, is invaluable as it better prepares the world for potential future attacks.

3.4. DARPA National Cyber Range

The US Government's Defence Advanced Research Projects Agency (DARPA) announced in 2008 the creation of a National Cyber Range (NCR). The project is intended to become a resource available to US military forces and government agencies for testing cyber programs. The project is still in progress with the latest news being the selection of two primary contractors to build and evaluate prototype ranges.

The NCR aims to simulate cyber attacks on computer networks and help develop strategies to defend against them. If implemented as planned, it will be able to test host security systems, local and wide area networks, and security tools by integrating or simulating them within an overall integrated system. The infrastructure of the NCR will allow the testing of new technologies and systems, such as new network protocols and other communications protocols, before their actual implementation.

Unfortunately, the project is unlikely to move past the prototyping phase. This bleak outlook is due to the fact that military and intelligence organizations, dissatisfied with the project's slow progress, want to build their own cyber ranges. For example, the US Navy wants to expand a small range at their Network Warfare Command and the US Air Force are planning a range dubbed "Cyber Safari" [25].

Even if DARPA's NCR does not move past prototype phase, its work there will be beneficial, especially if the insights gained can be integrated within the Navy and Air Force's respective cyber ranges. The obvious concern shown at DARPA's slow progress indicates that there is a strong desire for a large scale simulation infrastructure to test cyber defences.

3.5. France's Piranet

Piranet is one of the confidential defence plans of the French government [26-27]. Unlike other French plans that are geared specifically toward military crises such as a chemical attack (Piratox) or a nuclear attack (Piratome), Piranet is designed as the response to a major cyber attack on France's telecommunications and information systems infrastructure which impacts the military, public and private sectors. From 23-24 June 2010, the French government ran a live simulation exercise (Piranet 2010) to test the Piranet response.

The exact details of the exercise, along with its results are classified. However, the purpose of the exercise was to train government teams and to validate the emergency measures taken in order to decide if Piranet defences are still valid. The results of the exercise may be used to adjust the emergency response detailed in Piranet. It can be assumed that the exercises would have been conducted in a manner similar Cyber Storm, as the focus would have been on the officials' responses to attack scenarios instead of focusing on the technical side with network defence systems.

3.6. India's Divine Matrix

In March 2009 the Indian Army ran a war game called Divine Matrix [28]. The game simulated a notional nuclear attack by China on India in 2017. Beyond the more traditional war mechanics that were applied in the simulation; it is noteworthy that Divine Matrix simulated a massive cyber attack on India prior to the launch of any physical attacks. The cyber attacks had a kinetic result on the simulation, for example: the attacks disabled communication systems, damaged banking systems and

disabled power grids. The simulated attacks highlighted the need for cyber defence to senior Indian military leadership.

3.7. Concluding Remarks on Public Sector Research

Governments throughout the world are becoming increasingly concerned with CNO. This concern is demonstrated by an increase in training for defence against particular attack scenarios and the preparation of contingency plans. Some of the most interesting work conducted in the public sector has been done by the US Air Force who has been using virtual and constructive simulations to train for cyber attacks. The US Air Force has been experimenting with network defence simulations in SIMTEX, as well as focusing on the more global effect of cyber warfare by integrating cyber attack scenarios within existing war game simulators such as Modern Air Power. Furthermore, work in developing an experimental infrastructure to simulate cyber attack defences is on-going, as demonstrated in the efforts to develop the National Cyber Range as well as other military divisions' work to build their own cyber ranges. Finally, the reader should note that simulation and training for CNO is a resource intensive activity.

4. CONCLUSION

There has been considerable interest in the private and public sectors (including military forces) in the development of simulations of cyber attacks and CNO. Significant progress has already been made. Regrettably there appears to be very little coordination and cooperation across private sector organizations and governments in the development of effective cyber attack simulations. Some simulations share common traits and achieve similar results, which suggests that redundant work and research is being conducted.

Many of the simulations have had very different goals from each other. Costantini [3] and Cohen's work [5] were aimed at analyzing patterns and learning about cyber attacks, whereas CAPP [11] was aimed at highlighting the importance of cyber defence. Other simulations were entirely intended as training systems such as CAAJED [21], IWAR [22] and NetEngine [10]. Nevertheless, out of all the simulations discussed, very few attempted to integrate the technical details of cyber attacks with the global effect of CNO. Such integration, should it be developed, would result in an increased understanding and awareness of the threat cyber attacks pose to the world.

REFERENCES

[1] Chapman, I., Leblanc, S.P., Partington, A., "Taxonomy of Cyber Attacks and Simulation of their Effects" *Proceedings of the 2010 Military Modeling and Simulation Symposium (MMS'11)*, (2011).

[2] Kuhl, M. E., Kistner, J., Costantini, K., & Sudit, M. (2007). Cyber attack modeling and simulation for network security analysis. *Proceedings of the 2007 winter simulation conference* (pp. 1180-1188). http://www.informs-sim.org/wsc07papers/139.pdf.

[3] Costantini, K. C. (2007). *Development of a cyber attack simulator for network modeling and cyber security analysis*. Unpublished manuscript, Department of Industrial and Systems Engineering, Rochester Institute of Technology, Rochester, New York. Retrieved from https://ritdml.rit.edu/bitstream/handle/1850/5440/KCostantiniThesis10-2007.pdf?sequence=1

[4] Liljenstam, M., & Liu, J. (2006). Rinse: the real-time immersive network simulation environment for network security exercises (extended version). *SIMULATION, 82*(1), 43-59.

[5] Cohen, F. (1999). Simulating cyber attacks, defences, and consequences. *Computers & Security* (pp. 479-518). Elsevier Science Ltd.

[6] Park, J. S., Lee, J., K, H. K., Jeong, J., Yeom, D., & Chi S. (2001). Secusim: a tool for the cyber-attack simulation. *Information and Communications Security* (pp. 471-475). Heidelberg: Springer Berlin

[7] *Network simulation*. (2010). Retrieved from http://www.opnet.com/solutions/network_rd/modeler.html

[8] Sakhardande, R. R. (2008). *The use of modeling and simulation to examine network performance under denial of service attacks*. Unpublished manuscript, Department of Telecommunications, SUNY Institute of Technology, Utica, NY.

[9] Zhou, M., & Lang, S. (2003). A Frequency-based approach to intrusion detection. *Systemics, Cybernetics and Informatics, 2*(3), 52-56.

[10] Brown, B., Cutts, A., McGrath, D., Nicol, D. M., Smith, T. P., & Tofel, B. (2003). Simulation of cyber attacks with applications in homeland defense training. In E. M. Carapezza (Ed.*), Sensors, and command, control, communications, and intelligence (c3i) technologies for homeland defense and law enforcement ii* (pp. 63-71).

[11] FS-ISAC. (2010, June). *2010 capp exercise executive summary*. Retrieved from http://www.fsisac.com/files/public/db/p243.pdf

[12] Semantec, "W32.StuxNet dossier", Available from: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[13] Northrup-Gruman, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation". Available from: Northrup-Gruman, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation". Available from: http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

[14] *US Cyber Command Fact Sheet* (2011, February). Retrieved from http://www.stratcom.mil/factsheets/Cyber_Command/

[15] *Cyber Command Achieves Full Operational Capability*, US DOD News Release No. 1012-10, (3 November 2010), Retrieved from http://www.defense.gov/releases/release.aspx?releaseid=14030

[16] G. Conti and B. Surdu; "Army, Navy, Air Force, Cyber: Is it Time for a Cyberwarfare Branch of the Military;" Information Assurance

Newsletter, Vol. 12, No. 1, Spring 2009, pp. 14–18. Retrieved from: http://www.rumint.org/gregconti/publications/2009_IAN_12-1_conti-surdu.pdf

[17] Gettle, M. (2005, December 14). *Air force releases new mission statement.* Retrieved from http://www.af.mil/news/story.asp?storyID=123013440

[18] Griggs, S. (2010, June 16). *New officer course boosts cyberspace transformation.* Retrieved from http://www.keesler.af.mil/news/story.asp?id=123209671

[19] McBride, A. (2007, June). Air force cyber warfare training. *The Defense Standardization Program Journal*, 9-13.

[20] Hernandez, J. (2010, March 2). The *Human element complicates cybersecurity*. Retrieved from http://www.defensesystems.com/Articles/2010/03/11/Industry-Perspective-1-human-side-of-cybersecurity.aspx?Page=2

[21] Mudge, R. S., & Lingley, S. (2008). *Cyber and air joint effects demonstration (caajed).* Unpublished manuscript, Air Force Research Laboratory, Information Directorate, Rome Research Site, Rome, NY. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA481288&Location=U2&doc=GetTRDoc.pdf

[22] Lathrop, S. D., Conti, G. J., & Ragsdale, D. J. (2002). *Information warfare in the trenches*. Unpublished manuscript, US Military Academy, West Point, NY. Retrieved from http://www.rumint.org/gregconti/publications/iwar.doc

[23] Department of Homeland Security, National Cyber Security Division. (2006). *Cyber storm exercise report*. Retrieved from http://www.dhs.gov/xlibrary/assets/prep_cyberstormreport_sep06.pdf

[24] Department of Homeland Security, National Cyber Security Division. (2010). *Cyber storm exercise report*. Retrieved from http://www.dhs.gov/files/training/gc_1204738275985.shtm

[25] Fulghum, D. A. (2010, June 21). *Battle for cyber-range: military dumps darpa.* Retrieved from http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/asd/2010/06/21/03.xml&headline=Battle%20For%20Cyber-Range:%20Military%20Dumps%20Darpa%3E

[26] Naudon, M. (2010, June 25). *Exercice piranet 2010*. Retrieved from http://www.ssi.gouv.fr/IMG/pdf/2010-06-25_Communique_de_presse_Piranet_2010.pdf

[27] Morel, I. (2006, October). Les exercices de crise ssi. *Sécurité Informatique, 57*, Retrieved from http://www.dgdr.cnrs.fr/fsd/securite-systemes/revues-pdf/num57.pdf

[28] Singh, R. (2009, March 26). *Divine matrix: indian army fears china attack by 2017*. Retrieved from http://www.infowar-monitor.net/2010/02/divine-matrix-indian-army-fears-china-attack-by-2017/

Biographies

Sylvain (Sly) Leblanc is an Assistant Professor at the Royal Military College of Canada (RMCC). He obtained his Master's of Engineering in Software Engineering from RMCC in 2000, where he is also a doctoral candidate. Sly was a Canadian Army Signals Officer for over 20 years, where he developed his interest in computer network operations. His research interests are in computer security and computer network operations.

Ian Chapman is a defence scientist with the Defence Research and Development Canada Centre for Operational Research and Analysis in Ottawa, Canada. Mr. Chapman's work has included analytical support to a number of modeling and simulation activities at the Canadian Army Experimentation Centre and is now working with the Canadian Cyber Task Force to determine the effects of cyber attacks on military mission effectiveness.

Andrew Partington is in his final year of undergraduate studies, studying for his Bachelor of Engineering with Honors in Mechatronics Engineering at the University of Canterbury in New Zealand. He was a recent participant in a university exchange program, studying at Queen's University in Canada for a year in 2010. During the exchange he worked full time in the summer and part time during the school year at the Royal Military College of Canada researching computer network operations and simulations.

Melanie Bernier is a Defense Scientist with the Defence Research and Development Canada's Center for Operational Research and Analysis in Ottawa, Canada. She has experience in modeling and simulation of land forces requirements, concept development and experimentation, joint C4ISR, and computer networks. Most recently, she has been leading studies in force development for the cyber environment.