Challenges in Monitoring Cyberarms Compliance

Neil C. Rowe, U.S. Naval Postgraduate School, USA

Simson L. Garfinkel, U.S. Naval Postgraduate School, USA

Robert Beverly, U.S. Naval Postgraduate School, USA

Panayotis Yannakogeorgos, Air Force Research Institute, USA

ABSTRACT

A cyberweapon can be as dangerous as any weapon. Fortunately, recent technology now provides some tools for cyberweapons control. Digital forensics can be done on computers seized during or after hostilities. Cyberweapons differ significantly from other software, especially during development, and recent advances in summarizing the contents of storage media can locate possible cyberweapons quickly. Use of cyberweapons can be distinguished in the usual malicious Internet traffic by being aimed at targets associated with political, social, and cultural issues that are often known in advance, and those targets can then be monitored. Cyberweapons are relatively unreliable compared to other kinds of weapons because they are susceptible to flaws in software; therefore, cyberweapons require considerable testing, preferably against live targets. Thus, international "cyberarms agreements" could provide for forensics on cyberweapons and usage monitoring. Agreements also encourage more responsible cyberweapons use by stipulating attribution and reversibility. The authors discuss the kinds of international agreements that are desirable, and examine the recent interest of the U.S. government in such agreements.

Keywords: *Cyberarms Agreements, Cyberattacks, Cyberweapons, Forensics, Monitoring, Reversibility*

1. INTRODUCTION

Cyberweapons are digital objects that can be used to achieve military objectives by disabling key functions of computer systems and networks. They can be malicious software installed secretly through concealed downloads or deliberate plants by human agents, or they can be malicious data or maliciously delivered data as in denial-of-service attacks. Cyberweapons are a growing component in military arsenals (Libicki, 2007). Increasingly countries are instituting "cyberattack corps" with capabilities to launch attacks in cyberspace on other countries as an instrument of war, either alone or combined with attacks by conventional military forces (Clarke & Knake, 2010). Cyberattacks appeal to many military commanders. They seem to require fewer resources to mount since their delivery can be accomplished in small payloads such as malicious devices or packets that can be primarily delivered through existing

DOI: 10.4018/ijcwt.2011040104

infrastructure such as the Internet. They also seem "cleaner" than conventional weapons in that their damage is primarily to data and data can be repaired, although they are difficult to control and usually entail actions close to perfidy, something outlawed by the laws of war (Rowe, 2010). Cyberweapons can be developed with modest technological infrastructure, even by underdeveloped countries (Gady, 2010) by taking advantages of international resources. So there is a threat of cyberattacks from "rogue states" such as North Korea and terrorist groups that hold extreme points of view, as well as from countries with well-developed cyberweapons capabilities such as China.

Many information-security tools we use today to control threats and vulnerabilities with criminal cyberattacks (Brenner, 2010) help against the cyberweapon threat. Good software engineering practices in design and construction of software, access controls on systems and data, and system and network monitoring for suspicious activity all help. But they are insufficient to stop cyberattacks today because there are ways, albeit challenging, to subvert each of them, and the increasing complexity of cybersystems provides increasing opportunities for finding flaws in software. State-sponsored cyberattacks should be especially hard to prevent because states can exploit significant resources and can use them to develop highly sophisticated attacks. States will likely employ a variety of methods simultaneously to achieve a high probability of success, and will test them considerably more carefully than the hit-or-miss approach of most criminal attacks today. Such challenging state-sponsored cyberattacks will be difficult or impossible to defend against with current information-security defensive techniques.

2. APPROACH

What can be done against such threats then? We believe that countries must negotiate international agreements similar to those for nuclear, chemical, and biological weapons. Such agreements (treaties, conventions, protocols, and memoranda of understanding) (Croft, 1996) can stipulate the ways in which cyberweapons can be used, as for instance stipulating that countries use cyberweapons only in a counterattack to a cyberattack. Agreements can also stipulate policing of citizens such as "hacker" groups within a country, so that a nation cannot shift blame for cyberattacks and cyberweapons onto them. A few such agreements are in place today for cybercrime, but the growing threat suggests that it is time to plan out what such agreements will entail and how they should be enforced. As an example, the EastWest Institute in the U.S. recently proposed a cyberwar "Geneva Convention" (Rooney, 2011). Deterrence, a key aspect of nuclear weapons control, is not possible with cyberweapons because revealing capabilities significantly impedes their effectiveness.

Johnson (2002) was skeptical in 2002 of the ability to implement cyberarms control, citing the difficulty of monitoring compliance. But his arguments are less valid today. Cyberweapons are no longer a "cottage industry" but require significant infrastructure for finding exploits, finding targets, gaining access, managing the attacks, and concealing the attacks. This necessary infrastructure leaves traces even when concealed. The cyberweapon infrastructure needs to be increasingly complex because target software, systems, and networks are increasingly hardened and complex, and because vulnerabilities are being found and fixed faster than ever. Advances in network monitoring make it possible to detect coordinated attacks and remote control of one machine by another as in botnets, since botnets need aggregate effects to be useful to attackers, and aggregate effects can be detected with statistics. Digital forensics has advanced significantly since 2002, making it possible to find many useful things about digital artifacts. Anonymity and encryption techniques that attackers depend upon are easy to see and are good clues to something suspicious. Some techniques central for criminal cyberattacks today such as code obfuscation have little legitimate use and are good indica-