Chapter 58

# Cyber Warfare

**Anna Granova**
*Pretoria Society of Advocates*

**Marco Slaviero**
*SensePost Pty Ltd*

The times we live in are called the Information Age for very good reasons: Today information is probably worth much more than any other commodity. Globalization, the other important phenomenon of the times we live in, has taken the value of information to new heights. On one hand, citizens of a country may now feel entitled to know exactly what is happening in other countries around the globe. On the other, the same people can use the Internet to mobilize forces to overthrow the government in their own country.[1] To this end, the capabilities of the Internet have been put to use and people have become accustomed to receiving information about everyone and everything as soon as it becomes available. The purpose of this chapter is to define the concept of cyber warfare (CW), discuss their most common tactics, weapons, and tools, compare CW terrorism with conventional warfare, and address the issues of liability and the available legal remedies under international law. To have this discussion, a proper model and definition of CW first needs to be established.

October 20, 1969, marked the first message sent on the Internet,[2] and more 40 years on we cannot imagine our lives without it. Internet banking, online gaming, and online shopping and social media have become just as important to some as food and sleep. As the world has become more dependent on automated environments, interconnectivity, networks, and the Internet, instances of abuse and misuse of information technology infrastructures have increased proportionately.[3] Such abuse has, unfortunately, not been limited only to the abuse of business information systems and Web sites but over time has also penetrated the military domain of state security. Today this penetration of governmental IT infrastructures, including, among others, the military domain, is commonly referred to as *cyber warfare*. However, these concepts are not yet clearly defined and understood. Furthermore, this type of warfare is a multidisciplinary field requiring expertise from technical, legal, offensive, and defensive perspectives. Information security professionals are challenged to respond to this type of warfare issues in a professional and knowledgeable way.

## 1. CYBER WARFARE MODEL

The authors propose a model for CW by mapping important concepts regarding them on a single diagrammatic representation (see Figure 58.1). This aids in simplifying a complex concept as well as providing a holistic view on the phenomenon. To this end, this chapter addresses the

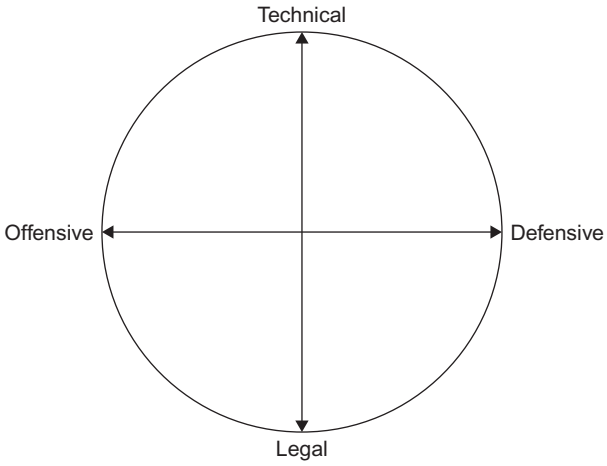


**FIGURE 58.1** A perspective on CW.

1. *Egypt: AP Confirms Government has Disrupted Internet Service* (2011), http://pomed.org/blog/2011/01/egypt-ap-confirms-government-has-disrupted-internet-service.html/, accessed on 09 April 2012.
2. *An Internet History* (2008), www.services.ex.ac.uk/cmit/modules/the_internet/webct/ch-history.html, accessed on 19 February 2008.
3. *Symantec Global Internet Security Threat Report Trends for July–December 07* (2008) Vol. 13, published April 2008 available at http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf, accessed on 21 April 2008.

**Computer and Information Security Handbook. DOI: http://dx.doi.org/10.1016/B978-0-12-394397-2.00058-1**

four axes of CW: technical, legal, offensive, and defensive, as depicted in Figure 58.1.

The technical side of CW deals with technical exploits on one side and defensive measures on the other. As is apparent from Figure 58.1, these range from the most destructive offensive strategies, such as a distributed denial-of-service (DDoS) attack or stuxnet, to various workstation emergency response teams, such as US-CERT.

Considered from a legal perspective, CW can range from criminal prosecutions in international courts to use of force in retaliation. Therefore, the four axes of CW continuously interact and influence each other, as will become clearer from the discussion that follows.

## 2. CYBER WARFARE DEFINED

The manner in which war is being conducted has evolved enormously,[4] and CW has not only been accepted as a new direction in military operations,[5] but also been incorporated into some of the top military forces in the world, with China implementing an CW policy as early as 1995,[6] with United States Cyber Command (USCYBERCOM) established in 2009,[7] followed by China in July 2010,[8] US Cyber Warfare Intelligence Center[9] unveiled in November 2010 and the Cyber Warfare Administration in Israel in breathed into life in 2012.[10] A number of definitions are relevant for the purposes of this chapter. Some authors[11] maintain that CW covers "the full range of competitive information operations from destroying IT equipment to subtle perception management, and from industrial espionage to marketing." If one regards the more "military" definition of CW, one could say that CW is "a subset of information operations"—in other words "actions taken to adversely affect information and information systems while defending one's own information and information systems."[12]

The UN Secretary-General's report on *Development in the Field on Information and Telecommunications in the context of International Security* describes CW as "actions aimed at achieving information superiority by executing measures to exploit, corrupt, destroy, destabilise, or damage the enemy's information and its functions."[13] This definition is very similar to one of the more recent and accepted definitions found in literature that states that CW is "actions taken in support of objectives that influence decision-makers by affecting the information and/or information systems of others while protecting your own information and/or information systems."[14] If one, however, looks at CW in purely a military light, the following technical definition seems to be the most appropriate: "The broad class of activities aimed at leveraging data, information and knowledge in support of military goals."[15]

In light of the preceding, it is clear that CW is all about information superiority because "the fundamental weapon and target of CW is information."[16] This being so, some authors[17] outline the basic strategies of CW as follows:

1. Deny access to information
2. Disrupt/destroy data
3. Steal data
4. Manipulate data to change its context or its perception

A slightly different perspective on the aims of CW is perhaps to see it as "an attack on information systems for military advantage using tactics of destruction, denial, exploitation or deception."[18] Since about 2008, however, the CW starting to cross over into the physical realm through one of its forms: cyber warfare, which can be defined as "*politically motivated hacking to conduct sabotage and espionage*".

With these definitions in mind, it is now appropriate to consider whether CW is a concept that has been created by enthusiasts such as individual hackers to impress the rest of the world's population or is, in fact, part of daily military operations.

4. Schmitt, "Wired Warfare-Workstation Network Attack and *jus in bello"* 2002 *International Review of the Red Cross,* 365.
5. Rogers "Protecting America against Cybeterrorism" 2001 *United States Foreign Policy Agenda,* 15.
6. Ball "Security Challenges", Vol. 7, No. 2 (Winter 2011), pp. 81–103, http://www.securitychallenges.org.au/ArticlePDFs/vol7no2Ball.pdf, accessed on 09 April 2012.
7. *Cyber Command Achieves Full Operational Capability* (2010) http://www.defense.gov/releases/release.aspx?releaseid=14030 accessed on 09 April 2012.
8. Branigan "Chinese army to target cyber war threat" (2010), http://www.guardian.co.uk/world/2010/jul/22/chinese-army-cyber-war-department accessed on 09 April 2012.
9. *Construction begins on first cyber warfare intelligence center* (2010), http://www.af.mil/news/story.asp?id=123204543accessed on 09 April 2012.
10. *Israel to Establish Cyber Warfare Administration* (2012), http://www.israelnationalnews.com/News/News.aspx/151713 accessed on 09 April 2012.
11. Hutchinson and Warren, *CW – Corporate Attack and Defence in a Digital World (2001) and XVIIII.*
12. Schmitt, "Wired Warfare-Workstation Network Attack and *jus in bello"* 2002 *International Review of the Red Cross* 365. See also the definition by Goldberg available on line at http://psycom.net/CWar.2.html.
13. UNG.A.Res A/56/164 dated 3 July 2001.
14. Thornton, R, *Asymmetric Warfare – Threat and Response in the 20-First Century* 2007.
15. Vacca, J. R., *Computer Forensics: Computer Crime Scene Investigation (2nd Edition)* Charles River Media, 2005.
16. Hutchinson and Warren, *CW – Corporate Attack and Defence in a Digital World (2001), p. xviiii.*
17. Hutchinson and Warren, *CW – Corporate Attack and Defence in a Digital World (2001) p. xviiii.*
18. Vacca, J. R., *Computer Forensics: Computer Crime Scene Investigation (2nd Edition)* Charles River Media, 2005.

## 3. CW: MYTH OR REALITY?

Groves once said: "... nowhere it is safe ... no one knows of the scale of the threat, the silent deadly menace that stalks the network."[19] With the growing risk of terrorists and other hostile entities engaging in missions of sabotaging, either temporarily or permanently, important public infrastructures through cyber attacks, the number of articles[20] on the topic has grown significantly. To understand the gravity of CW and its consequences, the following real-life examples need to be considered. At the outset, however, it is important to mention that the reason there is so little regulation (see checklist, "An Agenda For Action For Regulating High Level Cyber Warfare Strategies") of computer-related activities with specific reference to CW both on national and international planes is that lawyers are very reluctant to venture into the unknown. The following examples, however, demonstrate that CW has consistently taken place since at least 1991. One of the first CW incidents was recorded in 1991 during the first Gulf War, where CW was used by the United States against Iraq.[21]

In 1998 an Israeli national hacked into the government workstations of the United States.[22] In 1999, a number of cyber attacks took place in Kosovo. During the attacks the Serbian and NATO Web sites were taken down with the aim of interfering with and indirectly influencing the public's perception and opinion of the conflict.[23]

These cyber attacks were executed for different reasons: Russians hacked U.S. and Canadian websites "in protest" against NATO deployment,[24] Chinese joined the online war because their embassy in Belgrade was bombed by NATO,[25] and U.S. nationals were paralyzing the White House[26] and NATO[27] Web sites "for fun." In 2000, classified information was distributed on the Internet,[28] and attacks were launched on NASA's laboratories,[29] the U.S. Postal Service, and the Canadian Defense Department.[30] As early as 2001, detected intrusions into the U.S. Defense Department's Web site numbered 23,662.[31] Furthermore, there were 1300 pending investigations into activities "ranging from criminal activity to national security intrusions."[32] Hackers also attempted to abuse the U.S. Federal Court's database[33] to compromise the peace process in the Middle East.[34]

In 2002, incidents of cyber terrorism in Morocco, Spain, Moldova, and Georgia[35] proved once again that a "hacker influenced by politics is a terrorist," illustrated by more than 140,000 attacks in less than 48 hours allegedly executed by the "G-Force" (Pakistan)[36] . During this period, a series of convictions on charges of conspiracy, the destruction of energy facilities,[37] the destruction of telecommunications facilities, and the disabling of air navigation facilities,[38] as well as cases of successful international luring and subsequent prosecutions, were recorded.[39]

In the second half of 2007, 499,811 new malicious code threats were detected, which represented a 571% increase from the same period in 2006.[40] With two thirds

19. Lloyd, I. J., *Information Technology Law* Oxford University Press 181 (5th Edition) 2008.
20. Groves, The War on Terrorism: Cyberterrorist be Ware, *Informational Management Journal,* Jan-Feb 2002.
21. Goodwin "Don't Techno for an Answer: The false promise of CW."
22. *Israeli citizen arrested in Israel for hacking United States and Israeli Government Workstations* (1998) http://www.usdoj.gov/criminal/cybercrime/ehudpr.hgm(accessed on 13 October 2002).
23. Hutchinson and Warren, *CW – Corporate Attack and Defence in a Digital World (2001).*
24. Skoric (1999), http://amsterdam.nettime.org/Lists-Archives/net-time-1-9906/msg00152.html, (accessed on 03 October 2002).
25. Messmer (1999) http://www.cnn.com/TECH/computing/9905/12/cyberwar.idg/, (accessed on 03 October 2002).
26. *"Web Bandit" Hacker Sentenced to 15 Months Imprisonment, 3 Years of Supervised Release, for Hacking USIA, NATO, Web Sites* (1999), www.usdoj.gov/criminal/cybercrime/burns.htm (accessed on 13 October 2002).
27. *Access to NATO's Web Site Disrupted* (1999), www.cnn.com/WORLD/europe/9903/31/nato.hack/ (accessed on 03 October 2002).
28. Lusher (2000), www.balkanpeace.org/hed/archive/april00/hed30.shtml (accessed on 03 October 2002).
29. *Hacker Pleads Guilty in New York City to Hacking into Two NASA Jet Propulsion Lab Workstations Located in Pasadena, California* (2000), www.usdoj.gov/criminal/cybercrime/rolex.htm (accessed on 13 October 2002).
30. (2000) www.usdoj.gov/criminal/cybercrime/VAhacker2.htm (accessed on 13 October 2002).
31. www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/Cybercrime/International_conference/ConfCY(2001)5E-1.pdf (accessed on 9 October 2002).
32. Rogers, *Protecting America against Cyberterrorism* U.S. Foreign Policy Agenda (2001).
33. (2001) "Hacker Into United States Courts' Information System Pleads Guilty," www.usdoj.gov/criminal/cybercrime/MamichPlea.htm (accessed on 13 October 2002).
34. (2001) "Computer Hacker Intentionally Damages Protected Computer" www.usdoj.gov/criminal/cybercrime/khanindict.htm (accessed on 13 October 2002).
35. *Hacker Influenced by Politics is Also a Terrorist* (2002), www.utro.ru/articles/2002/07/24/91321.shtml (accessed on 24 July 2002).
36. www.echocct.org/main.html (accessed on 20 September 2002).
37. *Hackers Hit Power Companies* (2002) www.cbsnews.com/stories/2002/07/08/tech/main514426.shtml (accessed on 20 September 2002).
38. U.S. v. Konopka (E.D.Wis.), www.usdoj.gov/criminal/cybercrime/konopkaIndict.htm (accessed on 13 October 2002).
39. U.S. v. Gorshkov (W.D.Wash), www.usdoj.gov/criminal/cybercrime/gorshkovSent.htm (accessed on 13 October 2002).
40. *Symantec Global Internet Security Threat Report Trends for July–December 07* (2008) Vol. 13, published April 2008 available at http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf accessed on 21 April 2008 at p.45.

**An Agenda for Action for Regulating High Level Cyber Warfare Strategies**

Please see the following recommendations for regulating high level cyber warfare strategies (Check All Tasks Completed):

_____**1.** The President of the United States should task the National Office for Cyberspace (NOC) to work with appropriate regulatory agencies to develop and issue standards and guidance for securing critical cyber infrastructure, which those agencies would then apply in their own regulations.

_____**2.** The NOC should work with the appropriate regulatory agencies and with the National Institute of Standards and Technology (NIST) to develop regulations for industrial control systems (ICS).

_____**3.** The government should reinforce regulations by making the development of secure control systems an element of any economic stimulus package.

_____**4.** The NOC should immediately determine the extent to which government-owned critical infrastructures are secure from cyber attack.

_____**5.** The president should direct the NOC and the federal Chief Information Officers Council, working with industry, to develop and implement security guidelines for the procurement of IT products (with software as the first priority).

_____**6.** The president should task the National Security Agency (NSA) and NIST, working with international partners, to reform the National Information Assurance Partnership (NIAP).

_____**7.** The president should take steps to increase the use of secure Internet protocols.

_____**8.** The president should direct the Office of Management OMB and the NOC to develop mandatory requirements for agencies to contract only with telecommunications carriers that use secure Internet protocols.

of more than 1 million identified viruses created in 2007,[41] the continued increase in malicious code threats has been linked to the sharp rise in the development of new Trojans and the apparent existence of institutions that employ "professionals" dedicated to creation of new threats.[42] In 2008 it has been reported in the media that "over the past year to 18 months, there has been 'a huge increase in focused attacks on our [United States] national infrastructure networks …. and they have been coming from outside the United States.'"[43]

It is common knowledge that over the past 15 years, the United States has tried to save both manpower and costs by establishing a system to remotely control and monitor the electric utilities, pipelines, railroads, and oil companies all across the United States.[44] The reality of the threat of CW has been officially confirmed by the U.S. Federal Energy Regulatory Commission, which approved eight cyber-security standards for electric utilities, which include "identity controls, training, security 'parameters' physical security of critical cyber equipment, incident reporting and recovery."[45] In January 2008, a CIA analyst warned the public that cyber attackers have hacked into the workstation systems of utility companies outside the United States and made demands, which led to at least one instance where, as a direct result, a power outage that affected multiple cities took place.[46]

Furthermore, since 2007, there have been a number of high profile events, which can be categorized as cyber attacks. Estonia was first in line to suffer from this debilitating form of aggression: it unleashed a wave of DdoS attacks, where websites were swamped by tens of thousands of requests, which in turn disabled them by overcrowding the bandwidths for the servers running the websites of the Estonian government, political parties, half of media organizations and the top two banks.[47]

Russia was blamed for the Estonian cyber conflict which was caused by the removal of a statue of

41. *Symantec Global Internet Security Threat Report Trends for July–December 07* (2008) Vol. 13, published April 2008 available at http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf accessed on 21 April 2008 at p. 45.

42. *Symantec Global Internet Security Threat Report Trends for July–December 07* (2008) Vol. 13, published April 2008 available at http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf accessed on 21 April 2008 at p. 46.

43. Nakashima, E and Mufson, S, "Hackers have attacked foreign utilities, CIA Analysts says," 19 January 2008, available at www.washingtonpost.com/wp/dyn/conmttent/atricle/2008/01/18/AR2008011803277bf.html, accessed on 28 January 2008.

44. Nakashima, E and Mufson, S, "Hackers have attacked foreign utilities, CIA Analysts says," 19 January 2008, available at www.washington-post.com/wp/dyn/conmttent/atricle/2008/01/18/AR2008011803277bf.html, accessed on 28 January 2008.

45. Nakashima, E and Mufson, S, "Hackers have attacked foreign utilities, CIA Analysts says," 19 January 2008, available at www.washington-post.com/wp/dyn/conmttent/atricle/2008/01/18/AR2008011803277bf.html, accessed on 28 January 2008.

46. Nakashima, E and Mufson, S. (2008), "Hackers have attacked foreign utilities, CIA Analysts says," www.washingtonpost.com/wp/dyn/conmttent/atricle/2008/01/18/AR2008011803277bf.html, accessed on 28 January 2008.

47. Traynor "Russia accused of unleashing cyberwar to disable Estonia" (2007) http://www.guardian.co.uk/world/2007/may/17/topstories3.russia accessed on 19 April 2012.

significant importance to Russian people. The repeat of the showdown, but now with Georgia on the receiving end, was witnessed in 2008 when Georgia was literally blown offline during its military conflict with Russia.[48]

China also appears to be waging a persistent low-profile campaign against many foreign nations, such as Japan,[49] the United States[50] and the United Kingdom.[51] The United States themselves are not above suspicion: some experts hint that it might have been that country[52] that unleashed such a powerful "cyber weapon" as Stuxnet which impacted Iran's ability to conduct nuclear research.

With Duqu worm having been discovered on 01 September 2011, and showing similar capabilities as Stuxnet,[53] it is only a matter of time before one is able to find the country behind the worm by analyzing the motives behind the facility which will suffer its onslaught. The appropriate questions that then arise are: How can CW be brought about and how can one ward against it?

## 4. CYBER WARFARE: MAKING CW POSSIBLE

To conduct any form of warfare, one would require an arsenal of weapons combined with an array of defensive technologies as well as laboratories and factories for researching and producing both. As far as CW is concerned, three general strategies need to be considered: preparation, offensive strategies and defensive strategies.

### Preparation

Without arms, wars cannot be fought. Weapons are not constructed overnight and so in order to be prepared to enter any war, a state must have stockpiles of weapons ready to be deployed; CW is no different. Preparation will play a major role in CW as hostile acts occur in seconds or minutes, but the acts themselves are the culmination of many man-years worth of work.

In addition to training personnel and producing cyber weapons, the preparation stage also consists of a wide range of information gathering activities. Effective warfare is premised on knowledge of the opponent's weaknesses, and having extensive knowledge of an adversary's technology and networks prior to any hostilities is important for planning.

Preparation thus broadly consists of research, reconnaissance and vulnerability enumeration. The preparation phase never reaches a conclusion; ongoing research produces new tools, vulnerabilities and exploits, reconnaissance must continually discover new targets while removing stale targets, and vulnerability enumeration must keep track of new and old targets, while testing for recent vulnerabilities.

#### *Research*

CW does not require the infrastructure investment that physical arms do,[54] however it requires highly trained personnel to develop cyber weapons and the process of training to the required skill levels occupies a significant portion of activities prior to hostilities breaking out. In addition, once personnel have the necessary skills they need time to uncover vulnerabilities and turn those into usable weapons. These are separate jobs; the notion of vulnerability research as a separate discipline to exploit writing is growing especially as the continued fragmentation of applications and hardware forces extreme specialization. In the commercial information security market, vulnerability research and exploit writing are often separate tasks handed to different individuals, especially where memory corruption bugs are concerned.

The bug finders' skills tend towards quickly understanding how an application or system is built, how they often fail using common usage patterns and the ability to reverse engineer protocols quickly. Good bug finders are adept at automating this process. Their task, for example,

48. Danchev "Coordinated Russia vs Georgia cyber attack in progress" (2008) http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670 accessed on 09 April 2012, Tikk "Cyber Attacks Against Georgia: Legal Lessons Identified" (2008) http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf accessed on 09 April 2012.

49. "Japan parliament hit by China-based cyber attack" (2011) http://www.telegraph.co.uk/news/worldnews/asia/japan/8848100/Japan-parliament-hit-by-China-based-cyber-attack.html accessed on 09 April 2012.

50. "Identified Massive Global Cyberattack Targeting U.S., U.N. Discovered; Experts Blame China" (2011) http://www.foxnews.com/scitech/2011/08/03/massive-global-cyberattack-targeting-us-un-discovered-experts-blame-china/ accessed on 09 April 2012, Finkle "Cyber attack from China targets chemical firms: Symantec" (2011) http://www.msnbc.msn.com/id/45105397/ns/technology_and_science-security/t/cyber-attack-china-targets-chemical-firms-symantec/ accessed on 09 April 2012, Gorman "U.S. Report to Warn on Cyberattack Threat From China" (2012) http://online.wsj.com/article/SB10001424052970203961204577267923890777392.html accessed on 09 April 2012.

51. Foster "China chief suspect in major cyber attack" (2012) http://www.telegraph.co.uk/technology/news/8679658/China-chief-suspect-in-major-cyber-attack.html accessed on 09 April 2012.

52. Langner "Cracking Stuxnet, a 21st-century cyber weapon" (2011) http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html accessed on 09 April 2012, Waug "How the world's first cyber super weapon 'designed by the CIA' attacked Iran - and now threatens the world" (2011) http://www.dailymail.co.uk/sciencetech/article-2070690/How-worlds-cyber-super-weapon-attacked-Iran–threatens-world.html accessed on 09 April 2012.

53. Naraine "Duqu FAQ" http://www.securelist.com/en/blog/208193178/Duqu_FAQ#comments accessed on 09 April 2012.

54. Of the $707.5 billion requested for the U.S. Department of Defense 2012 budget, $159 million was earmarked for the Cyber Command.

is to find input that will cause a memory corruption to occur, after which the test case is handed to an exploit writer. Vulnerabilities are found at all layers and are introduced all stages of development, and vulnerability research strives to understand each component. Software bugs are not the only target; flaws in algorithms are highly valued and common misconfigurations often yield trivial exploits.

The exploit writer has extreme specialist knowledge of the inner working of the operating system on which the application runs, and is able to craft exploits that bypass operating system protections designed to thwart their exploits. With a working exploit in hand, the exploit writer then ensures it runs without crashing across a wide range of possible versions of the target software and operating system. The exploit will also often be obfuscated in some manner, to avoid detection. For the moment it serves to simplify cyber arms by thinking of them as exploits, but as we shall see, cyber weapons consist of further components.

The combined process of finding a bug and writing an exploit for it can take months. While not all vulnerabilities require that level of input, it is by no means extreme. Consider that cyber weapons are not simply just bugs and exploits; superficially, configuration and operational failures are prevalent but deeper issues in protocols and algorithms also exist.

### *Reconnaissance*

This phase of preparation focuses on identifying government organs, industries, infrastructure, companies, organizations and individuals that are potential targets. This is fed by a country's intelligence services, and overlaps with targets for physical warfare. In producing targets, information is gathered on the purpose of the targets, likely data that they store, technologies in use, network presence (on public or private networks) and channels by which the target could be engaged.

A discovery exercise is conducted on targets to determine which network services, if any, are accessible. Access to targets over the Internet is certainly not a requirement for CW but, for those that are, prior knowledge of their presence saves time when hostilities break out.

### *Vulnerability Enumeration*

With reconnaissance complete, the next preparation step is to discover vulnerable systems. Vulnerability scanning is a common activity in the commercial security industry, and numerous scanners exist. A scanner has a large database holding knowledge of tens of thousands of issues, as well as how to test for those issues. The kinds of tests vary; in some instances a test consists of simply checking a software version number extracted from a service banner, but in other tests more complex methods are required such as harmless exploits that confirm the vulnerability but do not take further action. By unleashing the scanner on a wide range of targets, a database of vulnerable machines can be saved prior to an CW.

Vulnerable systems are not the only benefit of wide scale scanning. Even a database of version numbers or technology types will improve targeting, for example when vulnerabilities for a system are discovered in the future.

The problem with scanners is that they are not subtle. They often test for issues unrelated to the technology on which the service runs, and protection mechanisms such as IDS are tuned to detect vulnerability scans. One improvement is scanning for specific issues across the target's networks which reduces the likelihood of detection, as well as masking tests to evade signature-based detection methods.

## Offensive Strategies

Scale is an important decision in deciding on an CW strategy. To extend the analogy of physical warfare, the strategic focus in CW could either be on small but highly experienced and trained tactical teams who are able to compromise targets at will, or to deploy an overwhelming number of moderately skilled operators. The analogy has flaws: whereas adding an extra operator in the physical realm increases the capabilities of that unit, adding extra CW operators past some point starts to see diminishing returns. The reason for this is that many CW operations can be automated and parallelized; additional *infrastructure* is often more valuable than additional personnel. Smaller teams decrease personnel and training costs, though they are more vulnerable to physical attacks against the teams.

A second consideration is the type of hostilities that CW covers. It will very likely be employed as a support to a kinetic war in the same way that ground troops value air cover. There is a second set of tactics that are *covert*, and these are akin to espionage. Regardless of whether the strategy is overt or covert, we refer to them a hostilities.

The arsenal of CW includes weapons of psychological and technical nature. Both are significant and a combination of the two can bring about astounding and highly disruptive results.

### *Psychological Weapons*

Psychological weapons include social engineering techniques and psychological operations *(psyops)*. Psyops

include deceptive strategies, which have been part of warfare in general for hundreds of years.

Sun Tzu, in his fundamental work on warfare, says that "All warfare is based on deception."[55] Deception has been described as "a contrast and rational effort … to mislead an opponent."[56] In December 2005, it became known that the Pentagon was planning to launch a US $300 million operation to place pro-U.S. messages "in foreign media and on items such as T-shirts and bumper stickers without disclosing the U.S. government as the source."[57]

Trust is a central concept and a prerequisite for any psyops to succeed. Traditionally, trust was vested in institutions and roles; a stranger in uniform might be afforded recognition based on the trust (if any) one has in the organization they are representing, without knowing them personally. Computer networks have, for some time now, been attacked by so-called "Social Engineers" who excel in gaining and exploiting trust, and cybercrime activities such as phishing rely on victims associating mere graphics on a website with the trust they invest in their bank.

However, this does not represent an exhaustive list of psyops. Psyops can also target the general population by substituting the information on well-trusted news agencies' Web sites as well as public government sites with information favorable to the attackers. A good example is where the information on the Internet is misleading and does not reflect the actual situation on the ground.

Today, social networks are highly efficient tools for spreading information. The instantaneous broadcast nature of micro-blogging sites such as Twitter mean that consumers rely more on social tools for obtaining information about current events than traditional media. In the heat of the moment, fact-checking quality decreases and the probability of inserting false information into social platforms increases. Social networks are also useful in guiding public conversations; Russia's legislative elections of 2011 saw automated software posting thousands of messages on Twitter in order to drown out opposition.[58]

The problem with psyops is that they cannot be used in isolation because once the enemy stops trusting the information it receives and disregards the bogus messages posted for its attention, psyops become useless, at least for some time. Therefore, technical measures of CW should also be employed to achieve the desired effect, such as DoS and botnet attacks. That way, the enemy might not only be deceived but the information the enemy holds can be destroyed, denied, or even exploited.

### Technical Weapons

There are non-subtle differences between weapons that exist in the physical realm and those that exist within the cyber realm, and the differences are useful to highlight. Bluntly put, there is no patch for an Intercontinental Ballistic Missile. To refine this further, a significant challenge facing a cyber army is that, while their attacks can occur virtually instantly, the target is able to respond as rapidly. The response may be to rollout patches for known issues, develop new patches for new vulnerabilities, employ perimeter defenses to filter out the attack traffic or simply disconnect the targeted system or network (perhaps, in the worst case scenario, even disconnect a country.)

A further challenge is the carrying of CW traffic. In the physical world, air and water provide the channels by which weapons are deployed, but in the cyber realm the path between two points is governed by a very different geography. It is a truism that in order to attack a network, an access channel extending from the attacker to the target is required. It could be a disconnected channel using flashdrives, or a highly technical and difficult operation such as the conquest of military satellites with ground-based resources or breaking into submarine cables, but the attacker must have a viable means for delivering their attack. While these complex or unreliable channels are possible, a more likely carrier for CW traffic is commercial Internet infrastructure supplied and maintained by global Internet Service Providers (ISPs), as they provide publicly accessible network links between countries around the world. In relying on commercial ISPs, attackers have the benefit of plausible deniability on the one hand, and on the other the ability to extend their reach into the commercial space of the target country, before attacking government and military targets.

CW attacks have the advantage that their implementation can be deployed long before any declaration of war. Whereas it is difficult to deploy physical armaments in preparation for detonating them near a target prior to a declaration of war, cyber attacks do not have the same limitation. Preparing attack launch pads either by compromising systems or by renting data center space can be performed months if not years in advance of attacks. When CW commences, the attacker is already well placed to wreak damage. A particularly effective force will compromise their target's supply chain, infusing equipment with backdoors years before they are used.

Rules of engagement present a further challenge. Traditional weapons are deployed at predetermined points in a conflict: artillery is seldom deployed when friendly

55. Sun Tzu, *Art of War.*
56. Thornton, R., *Asymmetric Warfare – Threat and Response in the Twenty-First Century,* 2007.
57. www.infowar-monitor.net/modules.php?op=modload&name=News&sid=1302, accessed on 28 September 2006.
58. http://www.guardian.co.uk/world/2011/dec/09/russia-putin-twitter-facebook-battles accessed on 29 February 2012.

troops are in the vicinity of the target, nuclear weapons may be a disproportionate response to a minor border skirmish and attacking schools or hospital without authorization may lie outside of a force's rules of engagement. Each armament has known side effects and its impact can be predicted; a commander in a physical war will understand which weapons are appropriate in each circumstance and deploy those that achieve their objectives while remaining within the constraints that are their policies and procedures. However, these norms have not been established publicly for CW, where *appropriate response* has yet to be defined. The dynamic nature of CW also means that, regardless of tools and techniques developed in the preparation phase, tools will be rapidly written during hostilities in reaction to new information or circumstances, and these could be trialed in the field while a conflict is active. Without perfect knowledge of exactly what a system controls or influences, unexpected consequences will be common in CW as the effects of an attack cannot be completely predicted.

The final significant difference between CW weapons and physical armaments is that their deterrence value is markedly different. Physical weapons demonstrate capability, which a cautious enemy will note. Developing defenses and counter-attacks against new weapons takes time in the real world, and so publicly exposing weapons capabilities can serve to avoid conflict. In the digital realm however, revealing one's weapons to an opponent simply highlights the areas they need to monitor, patch or upgrade. If an opponent provides evidence of working exploits against SoftwareX then, as a first line of defense, all of the target's machines running SoftwareX are moved behind additional layers and a plan is formulated to migrate away from SoftwareX. The defense can also perform their own investigation into SoftwareX, to determine the possible bug. By the time a conflict occurs, the revealed weapons are no longer useful. It has been shown in the commercial software exploit market that merely publishing seemingly innocuous descriptions of bugs can lead to experienced bug finders rapidly repeating the discovery without additional help. Demonstrating cyber capabilities is a confidence game in which a little skin is shown, in order to imply the strength of weapons that remain hidden. This is very susceptible to bluffing and subterfuge. With all this in mind, what do cyber weapons look like?

Previous work defined them as individual tools such as viruses, Trojans and so on. However, CW is fought at a larger scale than individual attacks, exploits and vulnerabilities. A commander on an CW battlefield is concerned with achieving objects such as disabling powergrids to support a kinetic attack on a facility. The commander firstly requires a team and infrastructure that is able to communicate and act in a distributed fashion; channeling attacks across lone routes or network links exposes a single point of failure, and attacks should be launched from a platform that is close in network terms to the target. This platform may be some distance from the command post. The weapons should be capable of working across multiple locations, and the payloads too must run in parallel and from multiple points in the network. Secondly, the commander must remain in control of attacks. For example, a worm that is unleashed against a target cannot indiscriminately attack targets on the public Internet as this would not help achieve the goal, and possibly result in collateral damage of systems unrelated to the opponent. Attacks would either be directly controlled by the commander through a command channel, or the attack would be self-limiting in terms of time or through built-in target detection. Examples of target detection are hardcoded addresses (when the reconnaissance phase was effective,) or a set of heuristics for determining at run-time whether a potential target should be attacked. This was seen in the Stuxnet attack, where the malicious code contained numerous heuristics to determine when it had finally migrated to the target SCADA installation. Until those heuristics were triggered, the program did nothing except attempt to migrate further. Lastly, a feedback loop that keeps the commander updated on whether the attack has succeeded is important. If the attack has a physical effect (for example, knocking out a powergrid), then the feedback loop would include forces on the ground. However, where the impact is virtual, then detecting attack success is not so clear cut. Consider the objective of disabling an opponent's logistics capability by preventing access to their logistics application through a deluge of traffic. Should the application become unresponsive from an attacker's perspective then it is not immediately apparent if the cause of the outage was a successful attack or due to the attack being detected and all the attacker's traffic blocked. Telemetry is vitally important.

Remember that CW is an "attack on information systems for military advantage using tactics of destruction, denial, exploitation or deception." The tactics by which the advantage is gained are determined by the weaknesses in the opponents systems, not the weapons in one's arsenal. This is important as it suggests that CW is not defined simply in terms of a set of tools; rather, the purpose or intent behind the deployment of a tactic is what defines a tactic to be part of an CW action. We shall see that so-called cyber weapons, in many circumstances, are called viruses, Trojans and the like when deployed by criminals or fraudsters. In that sense, the actual malicious components are less interesting as they are seldom unique to the field of CW and have been covered in this book already. The broader set of CW tools includes vulnerability databases, deployment tools, payloads and control consoles.

### Vulnerability Databases

The vulnerability database is the result of an effort to collect information about all known security flaws in software. From the outset, it is obvious this is a massive challenge as vulnerability information is generated by thousands of sources including software vendors, vulnerability researchers and users of the software. Public efforts exist to provide identifiers for security weaknesses in software applications, such as the MITRE Corporations' Common Vulnerabilities and Exposures (CVE) project, which defines itself as "dictionary of common names (CVE Identifiers) for publicly known information security vulnerabilities."[59] The CVE contains information about a particular vulnerability in a software product, but for CW this is only part of the required information. A truly useful CW vulnerability database will also include those opposing systems that have been discovered to exhibit a particular weakness. The weaknesses are not simply software vulnerabilities; in many cases misconfigurations lead to compromise, and these are not problems with the code but snags resulting from the manner in which the system was setup.

### Deployment Tools

Commonly seen in commercial malware where they are known as "droppers", deployment techniques are a separate beast from the payload that executes after compromise. Deployment occurs by exploiting a vulnerability, attacking a misconfiguration, spreading misinformation, spoofing communications, collusion or coercion. Stuxnet, for example, was deployed via four previously unknown vulnerabilities in Microsoft Windows, as well as through known network-based attacks. What made Stuxnet particularly interesting is that one infection mechanism was via USB flashdisks, as the target was presumed to not have public Internet connectivity.

Development of deployment tools occupies a large portion of the preparation phase, as discovered vulnerabilities and their exploits written form the basis for deploying malicious code. A stockpile of these tools aids an CW action, especially where tools take advantage of unknown flaws in software (termed "zero day", "0day", "0-day" or "oh-day").

### Payloads

Merely loading malicious code onto a target does not constitute a full attack. Seldom is compromise the sole CW tactic; rather, post-compromise is where the CW tactic is implemented. Payloads consist of the post-compromise logic, and can be swapped out depending on the intended tactic. In this way, deployment and payload are separate tools but combined to form a single attack. Potential actions by malicious code are covered elsewhere in the book, here we mention a sample of possible payloads that have been seen in examples of CW.

A DoS attack is an overt example of CW, in that its effects will be plainly visible to the target; an important system will no longer be accessible or usable. DoS attacks were amongst the first malicious tactics to be labeled as actual CW maneuvers in state-on-state disputes. In 2007, Estonia suffered a massive DoS attack that lasted three weeks, and interrupted financial and governmental functions, while in a dispute with Russia.[60] Whether the attack was conducted by organs of the Russian state has never been established; however, CW does not necessitate actions are conducted only by nation states. Standards for attribution are not clearly defined, as we shall see.

The adoption of Supervisory Control and Data Acquisition (SCADA) network-connected systems for the U.S. infrastructure, such as power, water, and utilities,[61] has made DoS attacks a lethal weapon of choice. Offline SCADA systems could have spectacular kinetic results. In 2010, a covert attack given the name Stuxnet was targeted at nuclear facilities in Iran. It succeeded in causing widespread damage by replacing control code on SCADA systems, and aimed to remain covert by feeding the operators false instrument information while the attack was underway.

### Control Consoles

In the commercial information security business, attack consoles are a known quantity. Software such as CORE IMPACT,[62] CANVAS[63] and Metasploit[64] provide interfaces that help the operator find vulnerabilities in target systems and launch exploits against those targets. The consoles ship with knowledge of hundreds of vulnerabilities, and include exploits for each one. The consoles also contain a multitude of payloads that can be attached to any exploit, that perform tasks such as account creation, command shell access or attacks against machines further in the network. An CW control console would contain the same elements as a commercial attack console, but also include the previously prepared vulnerability database as well as sport advanced telemetry to determine attack success.

59. http://cve.mitre.org/about/index.html, accessed on 10 March 2012.

60. Geers, K. (2008), *Cyberspace and the Changing Nature of Warfare*, BlackHat Asia 2008.

61. McClure, S., Scambray, J., and Kurtz, G. (2003), *Hacking Exposed: Network Security Secrets & Solutions,* 4th ed., McGraw-Hill/Osborne, 505.

62. http://www.coresecurity.com/content/core-impact-overview, accessed on 10 March 2012.

63. http://immunityinc.com/products-canvas.shtml, accessed on 10 March 2012.

64. http://www.metasploit.com/, accessed on 10 March 2012.

## Defensive Strategies

As far as prevention is concerned, experts agree that "there is no silver bullet against CW attacks."[65] In the US, defense against CW is split between two entities: the Department of Defense (DoD) is responsible for defending military resources, and the Department for Homeland Security (DHS) is responsible for protecting critical infrastructure. Purely in terms of military spending, the DoD requested $3.2 billion for cybersecurity in 2012, of which $159 million was intended for the U.S. Cyber Command (USCYBERCOM),[66] a military command who mission is to be the organization that "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."[67] From this mission statement, it is also clear that an offensive capability will be maintained. According to one military official, this was envisioned to be split approximately 85 percent defense and 15 percent offense.[68]

Without question, the defender's job is harder than the attackers in the environment that currently exists. This is not to say it is a truism; it is certainly possible to envision a world in which uniform security is applied throughout all connected networks, however that world does not exist today. The defender's dilemma from an CW perspective has multiple facets. Apart from the oft cited statement that a defender needs to cover all avenues of attack while the attackers needs only find a single vulnerability, CW also introduces the additional difficulty of defending networks that one potentially does not control. Would an CW defense command have full access to all critical infrastructure networks? This is unlikely; rather, individual actions would have to be delegated to administrators of those networks, who best know the ins and outs of their own networks.

For the most part, the attacks listed here are preventable and detectable. The problem facing a large target entity such as a sovereign nation is to coordinate its defense of many possible individual targets. Policies and procedures must be consistent and thoroughly followed. This is a mammoth task, given the heterogeneous nature of large computing systems. CW defense calls for rapid communication between all points worthy of defense and the central defense command.

Current solutions are of an organizational nature. Many developed countries have response teams such as the Computer Emergency Response Teams (CERT), but these deal only with technicalities of attacks. Higher-level involvement from government is required to act as a line of defense for CW. The U.S. DHS has forged a link with the private and public sector in the form of the US-CERT, with the blessing of a national strategy for cyber defense, and DHS coordinates with USCYBERCOM to ensure protection across military, government and critical infrastructure networks. In the U.K., a similar role is played by the National Infrastructure Security Co-ordination Centre.

South Africa, as an example country of the developing world, does not yet have a high-level commitment to digital defense; however, there are initiatives in the pipeline to address CW issues. A number of international efforts that aim at securing the Internet and preventing attacks such as the ones mentioned here have been implemented. One such initiative is the adoption of the European Convention of Cybercrime 2001, which deals with the commercial aspects of the Internet transactions. As far as the military aspects of CW are concerned, there have been calls from a number of countries, notably Russia, that the Internet be placed under control of the United Nations.[69]

One author suggests that, while completely excluding attackers is desirable, this may not be attainable, and so proposes that "the purpose of cyberdefense is to preserve [the ability to exert military power] in the face of attack,"[70] by concentrating on desirable qualities such robustness, system integrity and confidentiality. This is achieved by architecture decisions (air-gapped networks), policy positions (centralized planning including forensic abilities, decentralized execution), strategic analysis (determining the purpose of distributed attacks) and effective operations.

Key to any cyberdefense is attribution; without identifying the source of the attack one is unable to launch counterattacks. Attribution is rarely guaranteed except

65. Lonsdale, D. J., *The Nature of War and Information Age: Clausewitzian Future* at 140.

66. Miller, J.N., Statement to the House Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, *Hearing on the Department of Defense in Cyberspcae and U.S. Cyber Command*, March 16, 2011. Available at http://www.dod.mil/dodgc/olc/docs/testMiller03162011.pdf, accessed 11 March 2012.

67. U.S. Cyber Command Fact Sheet, http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf, accessed on 10 March 2012.

68. Holmes, E., "Donley Sets out Structure for Cyber Command", *Air Force Times*, February 26 2009.

69. (2003) *"Russia wants the UN to take control over the Internet,"* www.witrina.ru/witrina/internet/?file_body=20031118oon.htm, accessed on 10 May 2005.

70. Libicki, M.C., *Cyberdeterrence and Cyberwar*, Santa Monica, CA: RAND Corporation, 2009. http://www.rand.org/pubs/monographs/MG877 accessed on 29 February 2012.

when extremely simplistic markers are used. For example, using the source IP address of an attack does not imply that the owner of that addresses was aware of the attack. Botnets are typically built from thousands of vulnerable machines around the Internet and, while a machine may form part of an CW action, the owner cannot be punished militarily. Rather, the impact of the attack must be assessed in conjunction with information gleaned from other sources, in order to determine who the likely source was. Even then, the information may not be sufficient to point to state actors; industrial espionage or commercial attacks share many characteristics with CW, as we have already highlighted.

## 5. LEGAL ASPECTS OF CW

The fact that the Internet is, by definition, international implies that any criminal activity that occurs within its domain is almost always of an international nature.[71] The question that raises concern, however, is the degree of severity of the cyber attacks. This concern merits the following discussion.

### Terrorism and Sovereignty

Today more than 110 different definitions of terrorism exist and are in use. There is consensus only on one part of the definition, and that is that the act of terrorism must "create a state of terror" in the minds of the people.[72]

The following definition of "workstation terrorism" as a variation of CW is quite suitable: "Computer terrorism is the act of destroying or of corrupting workstation systems with an aim of destabilizing a country or of applying pressure on a government,"[73] because the cyber attack's objective, *inter alia,* is to draw immediate attention by way of causing shock in the minds of a specific populace and thus diminishing that populace's faith in government.

Incidents such as hacking into energy plants, telecommunications facilities, and government Web sites cause a sense of instability in the minds of a nation's people, thereby applying pressure on the government of a particular country; therefore, these acts do qualify as terrorism and should be treated as such. Factual manifestations of war, that is, use of force and overpowering the enemy, ceased to be part of the classical definition of "war" after World War I,[74] and international writers began to pay more attention to the factual circumstances of each case to determine the status of an armed conflict. This is very significant for current purposes because it means that, depending on the scale and consequences of a cyber attack, the latter may be seen as a fully fledged war,[75] and the same restrictions—for example, prohibition of an attack on hospitals and churches—will apply.[76]

CW may seem to be a stranger to the concepts of public international law. This, however, is not the case, for there are many similarities between CW and the notions of terrorism and war as embodied in international criminal law.

The impact of the aforesaid discussion on sovereignty is enormous. Admittedly a cornerstone of the international law, the idea of sovereignty, was officially entrenched in 1945 in article 2(1) of the United Nations (UN) Charter.[77] This being so, any CW attack, whatever form or shape it may take, will no doubt undermine the affected state's political independence, because without order there is no governance.

Furthermore, the prohibition of use of force[78] places an obligation on a state to ensure that all disputes are solved at a negotiation table and not by way of crashing of the other state's Web sites or paralyzing its telecommunications facilities, thereby obtaining a favorable outcome of a dispute under duress. Finally, these rights of nonuse of force and sovereignty are of international character and therefore "international responsibility"[79] for all cyber attacks may undermine regional or even international security.

### Liability Under International Law

There are two possible routes that one could pursue to bring CW wrongdoers to justice: using the concept of "state responsibility," whereby the establishment of a material link between the state and the individual executing the attack is imperative, or acting directly against the person, who might incur individual criminal responsibility.

#### *State Responsibility*

Originally, states were the only possible actors on the international plane and therefore a substantial amount of jurisprudence has developed concerning state responsibility. There are two important aspects of state responsibility

71. Corell (2002), www.un.org/law/counsel/english/remarks.pdf (accessed on 20 September 2002).
72. J. Dugard, International Law: A South African Perspective 149 (2nd ed. 2000).
73. Galley (1996), http://homer.span.ch/∼spaw1165/infosec/sts_en/ (accessed on 20 September 2002).
74. P. Macalister-Smith, Encyclopaedia of Public International Law 1135(2000).
75. Barkham, *Informational Warfare and International Law,* 34 Journal of International Law and Politics, Fall 2001, at 65.
76. P. Macalister-Smith, Encyclopaedia of Public International Law 1400 (2000).
77. www.unhchr.ch/pdf/UNcharter.pdf (accessed on 13 October 2002).
78. www.unhchr.ch/pdf/UNcharter.pdf (accessed on 13 October 2002).
79. *Spanish Zone of Morocco* claims 2 RIAA, 615 (1923) at 641.

that are important for our purposes: presence of a right on the part of the state claiming to have suffered from the cyber attack and imputation of the acts of individuals to a state.

Usually one would doubt that such acts as cyber attacks, which are so closely connected to an individual, could be attributable to a state, for no state is liable for acts of individuals unless the latter acts on its behalf.[80] The situation, however, would depend on the concrete facts of each case, as even an *ex post facto* approval of students' conduct by the head of the government[81] may give rise to state responsibility. Thus, this norm of international law has not become obsolete in the technology age and can still serve states and their protection on the international level.

Attribution in the context of CW, without somebody coming forward to claim responsibility for the attack, may prove to be a difficult, if not impossible, task because to hold a state liable one would have to show that the government had effective control over the attacker but, though its conduct, failed to curtail the latter's actions directed at another state and threatens international peace and security.[82]

As a result, even though many attacks emanate from China, for example, the Chinese government will only be responsible if it supported or at least was aware of the attacker and went along with that attacker's plans. Solid forensic investigation would therefore be required before there can be any hope in attributing responsibility.[83]

## *Individual Liability*

With the advent of a human rights culture after the Second World War, there is no doubt that individuals have become participants in international law.[84] There are, however, two qualifications to the statement: First, such participation was considered indirect in that nationals of a state are only involved in international law if they act on the particular state's behalf. Second, individuals were regarded only as beneficiaries of the protection offered by the international law, specifically through international human rights instruments.[85]

Individual criminal responsibility, however, has been a much more debated issue, for introduction of such a concept would make natural persons equal players in international law. This, however, has been done in cases of Nuremberg, the former Yugoslavia, and the Rwanda tribunals, and therefore,[86] cyber attacks committed during the time of war, such as attacks on NATO web sites in the Kosovo war, should not be difficult to accommodate.

What made it easier is the fact that in 2010, the Review Conference for the International Criminal Court introduced article *8bis* to the Rome Statute of the International Criminal Court ("ICC") which finally defined the crime of "aggression" as "the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a State, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations".[87]

There is no doubt that use of unilateral force which threatens universal peace is prohibited in international law.[88] The difficulty in holding an individual responsible is two-fold: confirming jurisdiction of the ICC over the accused and proving the intention to commit the crime covered by the Rome Statute the ICC administers.

First, only persons who are found within the territory of the state that is a signatory to the Rome Statute or such state's nationals may be tried before the ICC. Secondly, there may be difficulties with justification of use of the same terms and application of similar concepts to acts of CW, where the latter occurs independently from a conventional war. Conventionally, CW as an act of war sounds wrong, and to consider it as such requires a conventional classification. The definition of "international crimes" serves as a useful tool that saves the situation: arguably being part of *jus cogens*,[89] crimes described by terms such as "aggression," "torture," and "against humanity" provide us with ample space to fit all the possible variations of CW without disturbing the very foundation of international law. Thus, once again there is support for the notions of individual criminal responsibility for cyber attacks in general public international law, which stand as an alternative to state responsibility.

In conclusion, it is important to note that international criminal law offers two options to an agreed state, and it is up to the latter to decide which way to go. The fact that there are no clear pronouncements on the subject by an

80. M.N. Shaw, International Law 414 (2nd ed. 1986).
81. For example, in *Tehran Hostages Case (v.) I.C.J. Reports,* 1980 at 3, 34–35.
82. Huntley (2010) "Controlling the use of force in cyber space: the application of the law of armed conflict during a time of fundamental change in the nature of warfare" 60 Naval L. Rev. 1 2010.
83. Friesen (2009) "Resolving tomorrow's conflicts today: How new developments within the U.N. Security Council can be used to combat cyberwarfare" 58 Naval L. Rev. 89 2009.
84. J. Dugard, International Law: a South African Perspective (2nd ed. 2000), p. 1.
85. J. Dugard, International Law: a South African Perspective 1 (2nd ed. 2000), p. 234.
86. M.C. Bassiouni, International Criminal Law (2nd ed. 1999), p. 26.
87. Resolution RC/Res.6 http://www.icc-cpi.int/iccdocs/asp_docs/Resolutions/RC-Res.6-ENG.pdf accessed on 09 April 2012.
88. Green (2011) "Questioning the peremptory status of the prohibition of the use of force" 32 Mich. J. Int'l L. 215 2010–2011.
89. M.C. Bassiouni, International Criminal Law (2nd ed. 1999), p. 98.

international forum does not give a blank amnesty to actors on an international plane to abuse the apparent *lacuna,* ignore the general principles, and employ unlawful measures in retaliation.

## Remedies Under International Law

In every discussion, the most interesting part is the one that answers the question: What are we going to do about it? In our case there are two main solutions or steps that a state can take in terms of international criminal law in the face of CW: employ self-defense or seek justice by bringing the responsible individual before an international forum. Both solutions, however, are premised on the assumption that the identity of the perpetrator is established.[90]

### *Self-Defense*

States may only engage in self-defense in cases of an armed attack[91] which in itself has become a hotly debated issue.[92] This is due to recognition of obligation of nonuse of force in terms of Art.2(4) of the UN Charter as being not only customary international law but also *jus cogens*.[93]

Armed attack, however, can be explained away by reference to the time when the UN Charter was written, therefore accepting that other attacks may require the exercise of the right to self-defense.[94] What cannot be discarded is the requirement that this inherent right may be exercised only if it aims at extinguishing the armed attack to avoid the conclusion of it constituting a unilateral use of force.[95] Finally, a state may invoke "collective self-defense" in the cases of CW. Though possible, this type of self-defense requires, first, an unequivocal statement by a third state that it has been a victim of the attack, and second, such a state must make a request for action on its behalf.[96]

Therefore, invoking self-defense in cases of CW today, though possible,[97] might not be a plausible option, because it requires solid proof of an attack, obtained promptly and before the conclusion of such an attack,[98] which at this stage of technological advancement is quite difficult. The requirement that the attack should not be completed by the time the victim state retaliates hinges on the fact that once damage is done and the attack is finished, states are encouraged to turn to international courts and through legal debate resolve their grievances without causing more loss of life and damage to infrastructure. Since most states would deny any support of or acquiescence to the actions of its citizens in executing an attack, the more realistic court that one would turn to in pursuit of justice is the ICC.

### *International Criminal Court*

The International Criminal Court (ICC) established by the Rome Statute of 1998 is not explicitly vested with a jurisdiction to try an individual who committed an act of terrorism. Therefore, in a narrow sense, cyber terrorism would also fall outside the competence of the ICC.

In the wide sense, however, terrorism, including cyber terrorism, could be and is seen by some authors as torture.[99] That being so, since torture is a crime against humanity, the ICC will, in fact, have a jurisdiction over cyber attacks, too.[100]

Cyber terrorism could also be seen as crime against peace, should it take a form of fully fledged "war on the Internet," for an "aggressive war" has been proclaimed an international crime on a number of occasions.[101] Though not clearly pronounced on by the Nuremberg Trials,[102] the term "crime of aggression" is contained in the ICC Statute and therefore falls under its jurisdiction.[103]

90. Murphy (2011) "Mission Impossible? International law and the changing character of war" 87 Int'l L. Stud. Ser. US Naval War Col. 13 2011, (2011) Lewis "Cyberwarfare and its impact on international security" http://www.un.org/disarmament/HomePage/ODAPublications/OccasionalPapers/PDF/OP19.pdf accessed on 09 April 2012.
91. U.N.Charter art. 51.
92. Cammack (2011) "The Stuxnet worm and potential prosecution by the international criminal court under the newly defined crime of aggression" 20 Tul. J. Int'l & Comp. L. 303 2011.
93. M.Dixon, Cases and Materials on International Law 570 (3rd ed., 2000).
94. P. Macalister-Smith, Encyclopaedia of Public International Law 362 (2000).
95. Military and Paramilitary Activities in and against Nicaragua *(Nic. v. U.S.A.),*www.icj-cij.org/icjwww/Icases/iNus/inus_ijudgment/inus_ijudgment_19860627.pdf (accessed on 11 October 2002).
96. M.Dixon, Cases and Materials on International Law 575 (3rd ed. 2000).
97. Barkham, *Informational Warfare and International Law,* Journal of International Law and Politics (2001), p. 80.
98. otherwise a reaction of a state would amount to reprisals, that are unlawful; see also *Nic.* v. *U.S.A.* case in this regard, www.icj-cij.org/icjwww/Icases/iNus/inus_ijudgment/inus_ijudgment_19860627.pdf (accessed on 11 October 2002).
99. J. Rehman, International Human Rights Law: A Practical Approach 464–465 (2002).
100. Rome Statute of the International Criminal Court of 1998 art.7, www.un.org/law/icc/statute/english/rome_statute(e).pdf (accessed on 13 October 2002).
101. League of Nations Draft Treaty of Mutual Assistance of 1923, www.mazal.org/archive/imt/03/IMT03-T096.htm (accessed on 13 October 2002); Geneva Protocol for the Pacific Settlement of International Disputes 1924, www.worldcourts.com/pcij/eng/laws/law07.htm (accessed on 13 October 2002).
102. P. Macalister-Smith, Encyclopaedia of Public International Law 873–874 (1992).
103. Art.5(1)(d) of the Rome Statute of the International Criminal Court 1998, www.un.org/law/icc/statute/english/rome_statute(e).pdf (accessed on 13 October 2002).

Cyber crimes can also fall under crimes against nations, since in terms of customary international law states are obliged to punish individuals committing crimes against third states.[104] Furthermore, workstation-related attacks evolved into crimes that are universally recognized to be criminal and therefore against nations. P. Macalister-Smith, Encyclopaedia of Public International Law 876 (1992). Therefore, thanks to the absence of *travaux préparatoires* of the Rome Statute, the ICC will be able to interpret provisions of the statute to the advantage of the international community, allow prosecutions of cyber terrorists, and ensure international peace and security.

In practical terms the above will mean that a cyber attack will most probably be interpreted as part of "any weapon"[105] within the scope of the definition of "aggression" of the Rome Statute and the attacker will face the full might of the law as long as he/she is the national of the member state or finds him/herself within the physical territorial boundaries of the state that is party to the Rome Statute even though the attacker's conduct may not be enough to make the country of its nationality liable for what he/she did.[106]

### *Other Remedies*

Probably the most effective method of dealing with CW is by way of treaties. At the time of this writing, there has been only one such convention on a truly international level, the European Convention on Cybercrime 2001.

The effectiveness of the Convention can be easily seen from the list of states that have joined and ratified it. By involving such technologically advanced countries as the United States, Japan, the United Kingdom, Canada, and Germany, the Convention can be said to have gained the status of instant customary international law,[107] as it adds *opinio juris* links to already existing practice of the states.

Furthermore, the Convention also urges the member states to adopt uniform national legislation to deal with the ever-growing problem of this century[108] as well as provide a platform for solution of disputes on the international level.[109] Finally, taking the very nature of CW into consideration, "hard" international law may be the solution to possible large-scale threats in future.

The fact that remedies bring legitimacy of a rule cannot be overemphasized, for it is the remedies available to parties at the time of a conflict that play a decisive role in the escalation of the conflict to possible loss of life. By discussing the most pertinent remedies under international criminal law, the authors have shown that its old principles are still workable solutions, even for such a new development as the Internet.

## Developing Countries Response

The attractiveness of looking into developing countries' response to an CW attack lies in the fact that usually these are the countries that appeal to transnational criminals due to lack of any criminal sanctions for crimes they want to commit. For purposes of this chapter, the South African legal system will be used to answer the question of how a developing country would respond to such an instance of CW.

In a 1989 "end conscription" case, South African courts defined war as a "hostile contest between nations, states or different groups within a state, carried out by force of arms against the foreign power or against an armed and organised group within the state."[110] In the 1996 *Azapo* case, the Constitutional Court, the highest court of the land, held that it had to consider international law when dealing with matters like these.[111] In the 2005 *Basson* case, the Constitutional Court further held that South African courts have jurisdiction to hear cases involving international crimes, such as war crimes and crimes against humanity.[112]

A number of legislative provisions in South Africa prohibit South African citizens from engaging, directly or indirectly, in CW activities. These Acts include the Internal Security Intimidation Act 13 of 1991 and the Regulation of Foreign Military Assistance Act 15 of 1998. The main question here is whether the South African courts would have jurisdiction to hear matters in connection therewith. A number of factors will play a role. First, if the incident takes place within the air, water, or *terra firma* space of South Africa, the court would have jurisdiction over the matter.[113]

The implementation of the Rome Statute Act will further assist the South African courts to deal with the matter because it confers jurisdiction over the citizens who

104. P. Macalister-Smith, Encyclopaedia of Public International Law 876 (1992).
105. Article 8 *bis* 2(b) of the Rome Statute, http://www.icc-cpi.int/icc-docs/asp_docs/Resolutions/RC-Res.6-ENG.pdf acc3essed on 09 April 2012.
106. Schmitt (2011) "Cyber Operations and the *Jus in Bello*: Key Issues" 87 Int'l L. Stud. Ser. US Naval War Col. 89 2011.
107. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (accessed on 9 October 2002).
108. European Convention on Cybercrime of 2001 art. 23, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (accessed on 9 October 2002).
109. European Convention on Cybercrime of 2001 art. 45, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (accessed on 9 October 2002).
110. Transcription *Campaign and Another v. Minister of Defence and Another* 1989 (2) SA 180 (C).
111. *Azanian People's Organisation (AZAPO) v. Truth and Reconciliation Commission* 1996 (4) SA 671 (CC).
112. *State v. Basson* 2005, available at www.constitutionalcourt.org.za.
113. Supreme Court Act 59 of 1959 (South Africa).

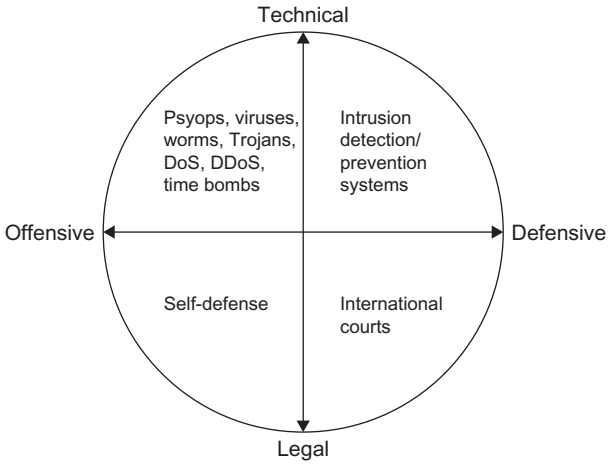


**FIGURE 58.2** Holistic view of CW.

commit international crimes. It is well known that interference with the navigation of a civil aircraft, for example, is contrary to international law and is clearly prohibited in terms of the Montreal Convention.[114]

A further reason for jurisdiction is found in the 2004 Witwatersrand Local Division High Court decision of *Tsichlas v. Touch Line Media*,[115] where Acting Judge Kuny held that publication on a Web site takes place where it is accessed. In our case, should the sites in question be accessed in South Africa, the South African courts would have jurisdiction to hear the matter, provided that the courts can effectively enforce its judgment against the members of the group.

Finally, in terms of the new Electronic Communications and Transactions (ECT) Act,[116] any act or preparation taken toward the offense taking place in South Africa would confer jurisdiction over such a crime, including interference with the Internet. This means that South African courts can be approached if preparation for the crime takes place in South Africa. Needless to say, imprisonment of up to five years would be a competent sentence for each and every participant of CW, including coconspirators.[117]

## 6. HOLISTIC VIEW OF CYBER WARFARE

This chapter has addressed the four axes of the CW model[118] presented at the beginning of this discussion: technical, legal, offensive, and defensive. Furthermore, the specific subgroups of the axes have also been discussed. For the complete picture of CW as relevant to the discussion at hand, however, Figure 58.2 places each subgroup into its own field.[119]

## 7. SUMMARY

This discussion clearly demonstrated that CW is not only possible, it has already taken place and is growing internationally as a preferred way of warfare. It is clearly demonstrated that successful strategies, offensive or defensive, are dependent on taking a holistic view of the matter. Information security professionals should refrain from focusing only on the technical aspects of this area, since it is shown that legal frameworks, national as well as international, also have to be considered. The prevailing challenge for countries around the globe is to foster collaboration among lawyers, information security professionals, and technical IT professionals. They should continue striving to at least keep the registry of CW arsenal and remedies updated, which may, in turn, incite adversaries to provide us with more material for research.

Finally, let's move on to the real interactive part of this Chapter: review questions/exercises, hands-on projects, case projects and optional team case project. The answers and/or solutions by chapter can be found in the Online Instructor's Solutions Manual.

## CHAPTER REVIEW QUESTIONS/EXERCISES

### True/False

1. True or False? The technical side of CW deals with technical exploits on one side and offensive measures on the other.
2. True or False? It is clear that CW is all about information superiority because "the fundamental weapon and target of CW is information.".
3. True or False? In addition to training personnel and producing cyber weapons, the preparation stage also consists of a wide range of information gathering activities.
4. True or False? CW does not require the infrastructure investment that physical arms do,[120] however it requires highly trained personnel to develop cyber weapons and the process of training to the required skill levels occupies a significant portion of activities prior to hostilities breaking out.
5. True or False? The reconnaissance phase of preparation focuses on identifying government organs, industries, infrastructure, companies, organizations and individuals that are not potential targets.

114. Montreal Convention of 1971.
115. *Tsichlas v. Touch Media* 2004 (2) SA 211 (W).
116. Electronic Communications and Transactions Act 25 of 2002.
117. Electronic Communication and Transaction Act 25 of 2002.
118. Supreme Court Act 59 of 1959 (South Africa).
119. Implementation of the Rome Statute of the International Criminal Court Act 27 of 2002 (South Africa).
120. Of the $707.5 billion requested for the U.S. Department of Defense 2012 budget, $159 million was earmarked for the Cyber Command.

## Multiple Choice

1. What type of scanning is a common activity in the commercial security industry, where numerous scanners exist?
   **A.** Qualitative analysis
   **B.** Vulnerabilities
   **C.** Data storage
   **D.** Vulnerability
   **E.** DHS
2. What is an important decision in deciding on a CW strategy?
   **A.** Network attached storage (NAS)
   **B.** Risk assessment
   **C.** Scale
   **D.** Subcomponents
   **E.** Bait
3. What type of weapons include social engineering techniques and psychological operations *(psyops)?*
   **A.** Organizations
   **B.** Fabric
   **C.** Psychological
   **D.** Risk communication
   **E.** Security
4. There are _____ differences between weapons that exist in the physical realm and those that exist within the cyber realm, and the differences are useful to highlight.
   **A.** Cabinet-level state office
   **B.** Non-subtle
   **C.** Infrastructure failure
   **D.** SAN protocol
   **E.** Taps
5. What type of database is the result of an effort to collect information about all known security flaws in software?
   **A.** Irrelevant
   **B.** Consumer privacy protection
   **C.** IP storage access
   **D.** Vulnerability
   **E.** Unusable

## EXERCISE

## Problem

How can organizations address advanced persistent cyber threats?

## Hands-On Projects

### *Project*

How are cyber-attacks carried out?

## Case Projects

### *Problem*

What targets can be attacked?

## Optional Team Case Project

### *Problem*

What are the implications of a cyber-attack?