2017

Challenges of civilian distinction in cyberwarfare

Rowe, Neil C.

Springer

Rowe, Neil C. "Challenges of civilian distinction in cyberwarfare." Ethics and Policies for Cyber Operations. Springer, Cham, 2017. 33-48.
http://hdl.handle.net/10945/65775

Chapter 3
Challenges of Civilian Distinction in Cyberwarfare

Neil C. Rowe

Abstract Avoiding attacks on civilian targets during cyberwarfare is more difficult than it seems. We discuss ways in which an ostensibly military cyberattack could accidentally hit a civilian target. Civilian targets are easier to attack than military targets, and an adversary may be tempted to be careless in targeting. Dual-use targets are common in cyberspace since militaries frequently exploit civilian cyber infrastructure such as networks and common software, and hitting that infrastructure necessarily hurts civilians. Civilians can be necessary intermediate objectives to get to an adversary's military, since direct Internet connections between militaries can be easily blocked. Cyberwarfare methods are unreliable, so cyberattacks tend to use many different methods simultaneously, increasing the risk of civilian spillover. Military cyberattacks are often seen by civilian authorities, then quickly analyzed and reported to the public; this enables criminals to quickly exploit the attack methods to harm civilians. Many attacks use automatic propagation methods which have difficulty distinguishing civilians. Finally, many cyberattacks spoof civilians, encouraging counterattacks on civilians; that is close to perfidy, which is outlawed by the laws of armed conflict. We discuss several additional problems, including the public's underestimated dependence on digital technology, their unpreparedness for cyberwarfare, and the indirect lethal effects of cyberattacks. We conclude with proposed principles for ethical conduct of cyberwarfare to minimize unnecessary harm to civilians, and suggest designating cyberspace "safe havens", enforcing reparations, and emphasizing cyber coercion rather than cyberwarfare.

Keywords Cyberwarfare • Civilians • Ethics • Distinction • Cyberattack • Networks • Dual-use • Reporting • Propagation • Perfidy • Infrastructure • Product tampering

N.C. Rowe (✉)
Computer Science Department, U.S. Naval Postgraduate School, Monterey, CA, USA, 93943
e-mail: ncrowe@nps.edu

M. Taddeo, L. Glorioso (eds.), *Ethics and Policies for Cyber Operations*,
Philosophical Studies Series 124, DOI 10.1007/978-3-319-45300-2_3

3.1 Introduction

Article 52 of the Additional Protocol I to the Geneva Conventions (1977) (ICRC 2015) is clear in stating principles regarding collateral damage that have been ratified by the majority of the world's countries:

> Article 52 – General protection of civilian objects
>
> 1. Civilian objects shall not be the object of attack or of reprisals. Civilian objects are all objects which are not military objectives as defined in paragraph 2.
> 2. Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.
> 3. In case of doubt whether an object which is normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling, or a school is being used to make an effective contribution to military action, it shall be presumed not to be so used.

These principles have been insufficiently respected for cyberspace as the world sees increasing planning for use of cyberspace by militaries (Geers et al. 2013; Dinniss 2012). The Stuxnet cyberattacks on Iran (Gross 2012) provide an example of a sloppy operation that insufficiently considered collateral damage to civilians. Around 10 million civilian machines were infected worldwide by a worm-based propagation that eventually found its way to targets in nuclear-processing facilities in Iran. The damage to the civilian machines was initially unclear, so quick removal was important. It costs at least $100,000 in U.S. dollars for the world to recognize, analyze, and find countermeasures for a new attack method, since it requires around 1000 h total by well-trained specialized personnel. Stuxnet was sufficiently novel that it probably cost $1,000,000 to analyze it, design signatures to recognize it, and develop methods to remove infected files and processes. Then deployment of the countermeasures in the form of antivirus software required additional downloads by users, which could however be bundled with other security updates so that the extra time for each user was about a second, for a total of 10,000,000 * (1/3600) hours * $100 per hour = $277,000.

Secondary costs were attempts to attribute the Stuxnet attacks, around $100,000 since this was not a high priority. More importantly, the reuse of Stuxnet attack methods in subsequent criminal cyberattacks (Kaplan 2011) probably resulted in 10,000 incidents worldwide probably requiring around $100 per incident to address, for an extra cost of $1,000,000 total.

Thus the total collateral damage of Stuxnet was at least $2.4 million. The international standard for insurance purposes is $50,000 per year of human life, so Stuxnet's collateral damage to civilians was equivalent to the taking of one average human life. The lesson of Stuxnet is that collateral costs, despite initial claims, can be significant with cyber operations.

Enforcing the distinction between military and civilian targets in warfare has a long history (Kinsella 2011). We agree with much of the legal analysis of (Brenner and Clarke 2011) but will focus more on the technical methods that lead to collateral damage in cyberwarfare. Technical threats can also have technical solutions.

3.2 Methods by Which Cyberwarfare Can Hit Civilians

We consider here the kinds of mechanisms of cyberwarfare spread to civilians. We shall use "civilian" in the informal sense of people not employed by militaries, realizing that there are many borderline cases (Kaurin 2007). For instance, people contracted to work for a military are not generally considered civilians. We use the term "cyberwarfare" to refer to any military operations accomplished primarily by the use of computers, networks, software, and digital data (Clarke and Knake 2010; Shakarian et al. 2013).

Nearly all methods proposed for cyberwarfare exploit flaws in software, and most methods are similar to those of cybercrime using malware, rootkits, and bot networks (Elisan 2012). We will use the term "cyberattack" to refer to all these methods.

3.2.1 Civilian Cyberspace Is Ubiquitous

Civilian objects, both hardware and software, are all over cyberspace. The vast majority of Internet traffic is civilian. All the hardware we depend on – desktop computers, laptop computers, tablets, mobile devices, and storage devices – is fundamentally civilian. Similarly, all the software we depend on – operating systems, network protocols, Web browsers, document processing, and security management – is also fundamentally civilian. When military organization use cyberspace, they predominantly build on top of this existing infrastructure with their own data, using methods like encryption to prevent their data from being read or interfered with by civilians and civilian software. That means that, for the most part, there are not many distinctively military targets in cyberspace. In fact, it is very difficult to restrict attacks to only military targets because they must circumvent so much civilian infrastructure.

To be sure, some military activities are critical enough to need special handling in the form of exclusively military hardware and software. Examples are weapons systems, command-and-control systems, military-vehicle controls, and weapons-production systems. But simply because they are critical to militaries, they are well-protected. They are hard to reach on the Internet, or they may be disconnected from it. So if a cyberattack goes astray, the odds are good that it will hit a civilian rather than a military target in cyberspace.

3.2.2 Civilians Are Easy Targets

Besides the difficulty of avoiding civilians in cyberspace, civilian targets are often easier to damage than military ones in cyberspace. Military organizations well understand the importance of maintaining their operations to keep their cyberspace

access, communications, and data safe. So they provide many layers of security for those systems in the form of access controls, cryptography, real-time monitoring for suspicious behavior, and deceptions to fool attackers.

Civilians have considerably lower standards of security. Commercial pressures encourage vendors of popular software (e.g. Microsoft Windows, Adobe Reader, Web browsers, and mail systems) to make their products unnecessarily complex. The rate of flaws in software is roughly proportional to the square of its size, so overly complex software runs high rates of bugs. For instance, the size of the minimum Microsoft Windows operating system on desktop computers, according to Microsoft, has gone from 18 megabytes in 1992 to 720 megabytes in 2000 and 20,000 megabytes in 2012. Little of this additional code is necessary for operation of the computer. The more bugs in software, the more vulnerabilities that can provide the basis for cyberattacks.

In addition, civilian targets are not prepared for cyberwarfare. The world has not seen a major cyberwar yet. Many civilians confuse cyberwar with cybercrime and expect that it will play out similarly. They expect, as in the case of cybercrime bank fraud, that someone will quickly and cheerfully refund their damage costs after a cyberwar and everything will be fine. However, cyberwar tends to target important assets, and tries to thoroughly disable them, so recovery from a cyberwar may be very slow.

This means that there are considerably greater opportunities for attacks on civilian targets than military targets, and the attacks can be simpler. Deliberate attacks on civilians are a violation of Article 52. However, when a country is greedy or desperate, they will be sorely tempted to attack civilian sites in cyberspace regardless of Article 52.

3.2.3 Civilians Can Be Desirable Targets

Another appealing thing about civilian targets is that such attacks can send political, social, or cultural messages that an attacker wishes to convey. By attacking U.S. banks, for instance, Islamic militants are making a statement about their advocacy of non-usurious banking under Sharia law. The attacking of military targets often does not send as clear a message, particularly the targets in big military organizations like those of the U.S. which engage in a large variety of activities all over the world. If war is just an extension of politics by other means, its message needs to be clear.

3.2.4 Dual-Use Targets Are Hard to Avoid

Because of the ubiquity of civilians in cyberspace, many military systems and artifacts are “dual-use” resources, or resources intended for both civilians and militaries. Dual-use resources can be legitimate military targets if they are justified

as per Article 52. An example would be a civilian mail server hosting a military command-and-control network, which could be attacked to prevent communications during a military operation. Another example would be the Global Positioning System (GPS) used to measure precise locations on the surface of the earth and whose disablement could greatly impede military operations, but could hurt civilian entities such as aircraft and emergency services. However, key issues are how much of the civilian system is of military use and how critical is that military use. Since civilian traffic on the Internet is so much larger than military traffic, the Internet must be described as almost entirely civilian. If the military use is small, it is hard to justify it as a military target according to the standards of Article 52.

It may be possible to attack only the military parts of a dual-use target to satisfy Article 52. For instance, one could modify a mail system by a cyberattack to lose military mail exclusively. But such attacks require detailed knowledge of the software target and are difficult to implement. Most cyberattacks, like most munitions, will engage in undiscriminating destruction because that is the easiest effect to get.

An ethical justification for attacking dual-use targets and harming civilians is that citizens often bear some responsibility for their government's actions. If a government has committed crimes with the support of its citizens, a cyberattack with broad international support against those citizens may be justified although it violates Article 52. However, as we discuss below, cyberattacks have peculiar side effects of being able to harm civilians in countries unrelated to a conflict. Stuxnet was an example with its widespread (albeit mild) damage, but any cyberattack that employs new methods will like cause some harm to the entire international community.

Side effects of disabling even small parts of the Internet can be significant. (Anonymous 2012) reports that the Chinese government's disabling of Domain Name Service (DNS) servers, to prevent Chinese citizens from reaching non-Chinese Web sites, led to failures all over the Internet since DNS servers are essential to Internet routing. If mere acts of censorship can hurt the Internet everywhere, a cyberwar could be much worse.

Dual-use targets can be deliberately constructed to be problematic to attack. For instance, a state can put their hospitals on the same network used by their military for command-and-control as a way to provoke international outcry if the network is attacked. This is an appealing tactic for weak states, although if it can be shown to be deliberate, they get no immunity under international law for their civilians being attacked. Still, it looks bad for the attacker.

3.2.5 Attacks Can Damage the Environment

Even if a target is exclusively military, side effects of a cyberattack may hurt the civilian environment. This is most likely with cyberattacks that cause physical damage to a target. Causing an explosion in a nuclear power station used by a submarine, for instance, can release nuclear materials into the environment. A precedent is

a cyberattack on an Australian sewage plant that caused a release of large amounts of sewage (Slay and Miller 2008). Matters are exacerbated by the tendency of military planners to think only in terms of military objectives, something that led during the Vietnam War in the 1960s to overuse of herbicides to reduce insurgent cover, destroying forests and causing health problems for the Vietnamese (War Legacies Project 2010).

3.2.6 Civilians Can Be Desirable Intermediate Steps

Stuxnet used many intermediate computers to get to the eventual target of Iranian nuclear facilities, and it is likely that future cyberattacks will be similar. That is because direct military-on-military cyberattacks will likely be blocked because militaries know most of the Internet sites of their possible adversaries already. So it is essential to get to a military cyber target indirectly through Internet sites that the target considers friendly or neutral. Civilian sites would generally be friendly. Unfortunately, this violates the Hague Convention Article V on neutrality:

> CHAPTER I: The Rights and Duties of Neutral Powers
> Article 1. The territory of neutral Powers is inviolable.
> Article 2. Belligerents are forbidden to move troops or convoys of either munitions of war or supplies across the territory of a neutral Power.
> Article 3. Belligerents are likewise forbidden to:
>
> (a) Erect on the territory of a neutral Power a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea;
> (b) Use any installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes, and which has not been opened for the service of public messages.

Cyberattacks designed to damage an adversary are a form of munition that sent to a target and then is triggered. Using intermediate Internet sites in neutral countries to convey such cyberattacks is moving munitions across the territory of a neutral power. Even cyberattacks to facilitate intelligence gathering would violate Article 3 on establishing installations on neutral territory not available for public messages (they cannot be public because then they could be found and removed by anti-malware software), and they would also likely function analogously to wireless telegraphy stations. (von Heinegg 2012) argues against this analysis, claiming that Internet sites that forward packets without processing them are like a global public service, and malicious packets cannot hurt these sites. This argument does not refute the danger of denial-of-service attacks where the volume of traffic is a weapon, and the volume could hurt the forwarding site too. In addition, packets get stored in many places on forwarding sites, and malware could conceivably get out and attack the forwarding site if it is vulnerable. More importantly, the only fast way stop an attack of unknown ultimate origin is to stop neutral sites from forwarding the attack by attacking them in turn, which could draw neutral countries unjustifiably into cyber warfare, just what the Hague Convention article is trying to prevent.

Victims could first try to contact the owners of the neutral site to stop the attack, but this is not always possible due to the required time and the possible lack of expertise at the neutral site.

3.2.7 The Unreliability of Cyberwarfare Encourages Overkill

Cyberwarfare methods tend to be unreliable because they depend on flaws and bugs in software and hardware. Flaws and bugs can disappear suddenly when their vendors find them. This does not bother cybercriminals, who if an attack fails, can just try another method or another target because they often do not care how or who they are attacking. But it is an issue for nation-states because they want to achieve more precise and certain effects on a few important targets. This means that cyberwarfare must use simultaneously several methods of rather different types, as Stuxnet did, to have a good chance of an effect. The methods must be of rather different types to reduce the chances that a failure of one significantly increases the chances of a failure of another. But having many methods of attack increases the chances of hitting civilians, because there are more possibilities for targeting mistakes.

3.2.8 Side Effects of Reporting the Attack Can Hurt Civilians

A serious form of collateral damage with cyberattacks is in the potential reuse of the attack in subsequent criminal attacks. Effective cyberwarfare generally requires surprise, achieved by finding and exploiting previously unrecognized flaws and bugs in software. It is especially important to find novel ones because known ones get fixed quickly. It is also especially important to find novel flaws and bugs because they are more likely to work, and failed attack attempts warn an adversary to harden their defenses and give them good clues as to how. So an adequate cyberwarfare attack requires a good number of novel methods to provide a good degree of success on a first strike.

These requirements mean that cyberweapons will be a good source of ideas for cybercriminals as well as the cyberwar units of other states. Certainly cybercriminals do prefer attacks that have been tested and shown to be effective. It was not long before some of the six attack methods of Stuxnet were being reused for cybercrime (Kaplan 2011).

Cybercriminals learn about new cyberattack methods from threat-alerting sites such as www.us-cert.gov, vulnerability databases like nvd.nist.gov, cybersecurity-related newsgroups like those at www.securityfocus.com, and attack-testing software like www.metasploit.com. While these sites are for defense and tend not to give many attack details, there are plenty of fee-based commercial sites that will give more details and even will sell you attack code. The monitoring that provides data for these sites is accomplished by a variety of automated tools (Hashim et al 2013),

and vendors compete fiercely to offer the most up-to-date notices of cyberattack methods. Why is such information posted if criminals can exploit it? The consensus of the information-security community is that it is more important to share information freely to enable finding countermeasures quickly than it is to conceal information to prevent a few additional attacks over a few days (TechRepublic 2005). Analysis can stop most cyberattack methods within days with a software modification or "patch" if a wide range of experts can contribute. However, not everyone gets the patch quickly since not everyone uses their systems everyday, and not all vulnerable systems are configured properly. Thus, any new cyberattack method will cause damage for several days to a good number of civilian systems, then continue causing damage at a gradually decreasing rate over a long period of time, and this will be the case regardless of the source of the attack.

Cybercriminals can also learn new cyberattack methods by monitoring the Internet directly. Tools called "sniffers" can look for particular kinds of suspicious traffic, and tools called "honeypots" can serve as decoy sites for collecting attacks. Even Twitter feeds can provide early warning of cyberattacks (Al-Qasem et al. 2013). So observant criminals can learn new attack methods even if no one else notices them.

3.2.9 Automatic Propagation of Cyberattacks

Some cyberattacks like Stuxnet reach their targets by propagating autonomously from one computer or device to another. Viruses (propagation of file infections) and worms (propagation of running processes) are the major examples. Autonomous propagation tries to circumvent normal controls on site access, often through vulnerabilities in software. Automatic propagation is appealing for cyberattacks because the attack can grow fast: The more sites and files are attacked, the more launching pads for further attacks, and the more subsequent attacks. This multiplies the effect of the initial attack quickly, and overwhelming force applied quickly is a key goal of military operations. Even if there are a limited number of ultimate targets as with Stuxnet, propagation to many sites increases the chances of reaching a target and the speed of getting there.

Civilian sites are good places from which to autonomously propagate an attack because civilian systems have fewer controls than military systems. But even if an ethical military planner tries hard to confine the propagation to military systems, this may fail because automatic attacks cannot easily distinguish what they are attacking. Cyberattack code needs to be small to sneak past defenses, and does not have much room to carefully analyze what it is attacking. Typically viruses and worms just scan systems for neighbor systems and go after all of them. Matters can get ugly if military systems have "backdoor" connections to civilian systems for purposes such as software updates. Civilian sites can also be connected to military sites because someone on the military site did not know what they were; sites rarely describe themselves internally, and even when they do, it is not placed consistently. Furthermore, just because a site has many military neighbors does not mean that it

does warfighting, since many military hospitals and public-relations sites have such connections, and conversely, many contractors with ".com" sites in the U.S. directly support the military. So one cannot judge whether a site is military or civilian easily, certainly not solely by its IP address or site-owner registration in the Regional Internet Registries such as ARIN.

Another serious danger of automatic propagation of viruses and worms is the difficulty of turning them off. They are like land mines that are committed to actions independent of the context, and they usually have no respect for ceasefires or surrenders since there is little room in their small packages for a communications receiver (and having such a receiver would make them easier to detect anyway). Continuing hostilities after a ceasefire or surrender are explicitly prohibited by the laws of war, so it will be important to stop viruses and worms then.

3.2.10 Spoofing of Civilians by Militaries

One more way in which civilians can be hit by cyberwarfare is when adversaries "spoof" (impersonate) to get past defenses. Since military sites block direct connections from adversaries, it can be effective for an adversary to pretend they are civilian by just modifying their source address rather than going through intermediate sites. Standard network protocols do not allow address modification, but an adversary can design their own protocols. Spoofing is useful with denial-of-service attacks such as those against Georgia in 2008 (USCCU 2009)

If a victim of a spoofed attack counterattacks, their counterattack will likely go to the spoofed address, causing civilian damage if a civilian was spoofed. Counterattacking is a natural human impulse that is hard for many victims to resist even if they are not sure who they are counterattacking. But careless counterattacking can easily do more harm than the original attack.

Spoofing of civilians by militaries is specifically prohibited by the laws of war under the name "perfidy". That is because spoofing of civilians increases disbelief in civilian status and increases the risk of legitimate civilians being harmed. Here is the relevant part of the Additional Protocol I of the Geneva Conventions. Note that perfidy need not risk killing someone by these conventions, just that it "injure" the adversary.

> Article 37 – Prohibition of perfidy
>
> 1. It is prohibited to kill, injure or capture an adversary by resort to perfidy. Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence, shall constitute perfidy. The following acts are examples of perfidy:
>
> (a) the feigning of an intent to negotiate under a flag of truce or of a surrender;
> (b) the feigning of an incapacitation by wounds or sickness;
> (c) the feigning of civilian, non-combatant status; and
> (d) the feigning of protected status by the use of signs, emblems or uniforms of the United Nations or of neutral or other States not Parties to the conflict.

2. Ruses of war are not prohibited. Such ruses are acts which are intended to mislead an adversary or to induce him to act recklessly but which infringe no rule of international law applicable in armed conflict and which are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law. The following are examples of such ruses: the use of camouflage, decoys, mock operations and misinformation.

Most cyberattacks also rely on a special kind of spoofing, impersonation of routine software by malicious software. That is because there are many defenses against attempts to subvert computers and devices: security kernels, hash and parity values computed on digital objects, anti-malware scanners, intrusion-detection systems, and software-based security-policy implementations. These countermeasures make it difficult to attack machines and software directly. So the only good hope is to subvert the civilian software of those machines. But when done to achieve military objectives, the software is then masquerading as a neutral party when it is in fact a tool of a military cyberattack. So subversion of civilian software is a form of perfidy and is outlawed by international law (Rowe 2013). Some cases are more obvious than others, such as modifying air-operations software to confuse locations of hospitals with locations of military units and thereby cause targeting of hospitals.

Subversion of software may be easier to understand as a form of product tampering. Tampering with commercial products by third parties is illegal in nearly all countries because a modified product can harm a consumer. In the U.S. this is a form of "malicious mischief" and there are serious penalties. Software, as an easily modifiable product, needs especially to trusted to be free of tampering. Most software vendors make customers sign "end-user license agreements" to agree not to modify the software because of its dangers as well as their own interest in controlling variations on the software. So the necessary modifications of software to accomplish cyberattacks violate domestic law in most countries as well as international law.

3.2.11 Psycholfogical Damage

Psychological consequences on civilians of their military being cyberattacked can be significant because the technology is mysterious and provides grounds for irrational fear. If major systems stop working, civilians will wonder what other systems will also stop working soon. This irrational fear can also affect the cyberattacking country because citizens will think their military is cyberattacking some serious threat. Many have written about the irrational fear of terrorism that has gripped the U.S. in recent years (Kimmel and Stout 2006) which has led to abuses of privacy in cyberspace (Angwin 2014).

3.3 Intensifiers for Collateral Damage

In this section we discuss some additional factors at play in civilian collateral damage of cyberattacks.

Military organizations expect that their technology may be damaged during conflict. For their cyber assets, they have extensive backup plans including both hardware and software replacements, including backup sites from which copies can be downloaded. Military organizations also have well-developed contingency plans for when they lose assets including communications. Civilians, on the other hand, are inadequately prepared for the collateral damage that can occur with cyberwarfare. Businesses have plans, but depend too much on legal remedies designed for cybercrime (such as suing someone) instead of hardening their systems, and this will be little help if they are hurt during major sabotage activities in cyberwarfare by countries with which their country does not share tort law. Home-computer and mobile-device users have little protection against cyberattacks since many backup sporadically if at all. They depend extensively on a narrow set of options for finding out about the world (like television and the Internet) that could easily be disabled during cyberconflict. That suggests that collateral damage to civilians will be more serious and long-lasting than the damage to military systems during cyberwarfare.

A related factor is that it is often harder for civilians to repair cyberattack damage than it is for militaries. Civilians often lack training to respond to cyber problems adequately since the technology is changing rapidly and few people, even the developed world, can keep up to date with it. In the less-developed world, fewer people still understand the technology, and a cyberattack on a less-developed country may leave it damaged for years unless it gets extensive outside assistance.

Some military apologists have suggested that cyberspace is a new isolated domain of conflict much like outer space and the depths of oceans, so that cyberwarfare is unlikely to have many consequences for civilians. This may have been true 20 or more years ago, but is less true today due to the increasing ubiquity of digital technology. Food, shelter, jobs, and other basic necessities are heavily dependent on digital technology in most countries. Our social infrastructure of power, transportation, financial services, commerce, medicine, and communications is heavily dependent on it as well, and everything is interconnected. Use of digital technology and cyberspace is no longer optional, and thus collateral damage can easily have consequences for everyone.

Another claim often made by military apologists is that cyberwarfare will be bloodless. However, all effective weapons can hurt and kill people, and cyberweapons are no exception; explosions are not the only way to kill people. Analysis of the U.S. invasion and occupation of Iraq 2003–2013 showed surprising numbers of violent civilian deaths, estimated at 600,000 in the first 3 years (Burnham et al 2006) due to the increased lawlessness in the country in that time. In addition, the crippling of the civilian infrastructure resulted in at least 100,000 additional deaths (Hagopian et al 2013). This was despite a swift military victory in the initial weeks. Cyberwarfare could be even more likely to damage civilian infrastructure.

3.4 Towards Ethical Principles for Cyberwarfare That Minimize Collateral Damage

Despite all these dangers, cyberwarfare can be conducted in ways that greatly minimize the collateral damage to civilians.

3.4.1 General Principles

To provide guidance in designing policies, and eventually laws, that could help reduce the danger of collateral damage, we propose the following principles.

- Avoid deliberate attacks on preponderantly civilian targets under any circumstances, no matter what the incentive. Military attack and defense should involve only military personnel.
- Avoid dual-use targets as much as possible, and proportionately to the degree to which they are civilian. A rule of thumb is that anything whose proportion of military use is less than that of the domestic economy of the victim state (4 % for the U.S.) can be treated as entirely civilian.
- Minimize propagation of cyberattacks through civilian cyberspace during attack setup and control, since propagation alone causes damage and can violate neutrality of nation-states.
- Avoid autonomous propagation of the cyberattacks by methods such as viruses and worms, since they are difficult to control and stop.
- Design cyberattacks so their methods cannot be easily reused by cybercriminals, as by obfuscating (deliberately complicating) the code.
- Prefer to attack specialized military hardware and software that is not used by civilian systems.
- Acknowledge responsibility for the attack and make its purpose clear, to achieve desired effects and avoid scapegoating innocent civilians.
- Either make the attack highly effective so it cannot be blamed on civilian incompetence, or conceal it well so criminals won't find it.
- Minimize the number of cyberattack methods to reduce the chances of reuse by cybercriminals.
- Attack only countries that have the resources to investigate it.
- Avoid perfidious attacks that subvert civilian infrastructure and could encourage mistrust of civilians and civilian artifacts.

3.4.2 Partitioning of Cyberspace

Another principle that will help reduce collateral damage is to separate the arena of cyberwarfare better from civilian activities. It is important to designate and respect cyber "safe havens" analogous to those for refugees in conventional conflicts (Geiss and Lahmann 2012). These would be designated unacceptable targets for cyberwarfare such as medical systems, power systems, banking systems, Google servers, Microsoft Update, and personal Web pages. Since these are almost exclusively civilian, it is hard anyway to justify them as military targets. However, dual-use entities shared by military and civilian users such as mail systems and databases could be legitimate military targets under occasional and carefully justified circumstances, and they should not be included in the "safe havens". We are starting to see some ideas about how to plan cyberattacks to limit collateral damage by trying to carefully identify characteristics of targets (Raymond et al 2013), though one can be skeptical of the ideas that do not take into account possible deception by an adversary, an essential part of military operations.

Partitioning of military cyberspace from civilian cyberspace is technically feasible in large part though there have not been strong incentives for it previously. Segregation need not be physical (accomplished by separate hardware). Separation can be "logical", meaning that military data and network communications are carried through different software mechanisms. Recent work has developed extensive technology for "virtual machines" and "cloud computing" that can allow software to execute in an environment well separated from a host environment so that viruses and worms cannot get out to the host environment (Pearce et al. 2013). Military systems have often pioneered the necessary technology.

3.4.3 Reparations

Cyberwarfare can cause significant damage. If cyberattacks are unprovoked, the laws of war should apply and enforce reparations for the damage. Reparations for cyberattacks can be assistance, perhaps through a third party, in repairing the damaged hardware, software, and data. The assistance of the attacker will often be required since often only the attacker knows exactly what was attacked and damage can be hard to see. An important justification for reparations is the deterrent effect they have on future cyberattacks, and deterrence is often the primary reason for having a military. For example, reparations should be due to Iran for the unprovoked cyberattack of Stuxnet, particularly since Iran was not at war with any country at the time.

3.4.4 A Role for Cyber Coercion

Since cyberwarfare methods are flexible, it is reasonable to consider more limited forms of cyberconflict as alternatives. Cyberconflict short of warfare has been termed "cyber coercion" (Flemming and Rowe 2015) and may suffice to resolve many conflicts. An example could be when an aggressor state prepares for a regional military dispute by sending ships to the area, but discovers that the command-and-control systems for those ships no longer function, and receives a message from an adversary telling them to back off; the induced system malfunction would function as coercion with the threat of further consequences for the aggressor state. Cyber coercion does not need to significantly impact a state's ability to wage war, as does conventional warfare; it suffices to provide a demonstration of capabilities since cyberattacks can often be scaled up.

Future warfare is likely to see many forms of cyber coercion. However, it has some disadvantages compared to conventional conflict. It may not be noticed by the victim unless it is strong enough, as it may be confused with normal system problems. At the other extreme, the victim may escalate the conflict after cyber coercion to demonstrate their own resolve, leading to the cyberwarfare that coercion was intended to avoid. Cyber coercion could unfairly target civilians just as much as full cyberwarfare unless the principles given above are followed. Nonetheless, in many cases cyber coercion may be a more focused and less problematic method of cyber influence short of cyberwarfare.

3.5 Conclusions

States wishing to go to war often provide incomplete justifications that insufficiently consider the costs to civilians involved in the conflict. Citizens should be made more aware of what the likely consequences are. Modern warfare has increasingly emphasized high-technology and infrastructure targets (Smith 2002). But for the new arena of cyberspace, incomplete arguments for offensive cyber operations are especially common, and possible consequences have been insufficiently understood and appreciated. This chapter has argued there are many ways, both overt and subtle, in which civilians can be hurt by cyberconflict, but there are ways to reduce such damages. Civilian distinction is only one of several ethical problems that need to be addressed in cyberwarfare, however (Rowe 2015).

Acknowledgements The views expressed are those of the author and do not represent the U.S. Government. This work was supported by the U.S. National Science Foundation under the Secure and Trustworthy Cyberspace program.

References

Al-Qasem, I., S. Al-Qasem, and A. Al-Hammouri, 2013. *Leveraging online social networks for a real-time malware alerting system*. In: Proceedings of the 38th IEEE conference on local computer networks, Sydney, AU, October, 272–275.

Angwin, J. 2014. *Dragnet nation: A quest for privacy, security, and freedom in a world of relentless surveillance*. New York: Times Books.

Anonymous. 2012, July. The collateral damage of Internet censorship by DNS injection. *ACM SIGCOMM Computer Communications Review*, 42(3):22–27.

Brenner, S., and L. Clarke. 2011. *Civilians in cyberwarfare: Casualties*. http://works.bepress.com/susan_brenner/3. Accessed 1 Nov 2011.

Burnham, G., R. Lafta, S. Doocy, and L. Roberts. 2006, October 11. Mortality after the 2003 invasion of Iraq: A cross-sectional cluster sample. *The Lancet*, 368(9545):1421–1428.

Clarke, R., and R. Knake. 2010. *Cyber war: The next threat to national security and what to do about it*. New York: HarperCollins.

Dinniss, H. 2012. *Cyber warfare and the laws of war*. Cambridge: Cambridge University Press.

Elisan, C. 2012. *Malware, rootkits, and botnets: A beginner's guide*. New York: McGraw-Hill Osborne.

Flemming, D., and N. Rowe. 2015. *Cyber coercion: Cyber operations short of cyberwar*. In: Proceedings of the 10th international conference on cyber warfare and security, Skukuza, South Africa, March.

Geers, K., D. Kindlund, N. Moran, and Rachwald. 2013. *World War C: Understanding nation-state motives behind today's advanced cyber attacks*. http://www.FireEye.com. Accessed 7 Apr 2013.

Geiss, R., and H. Lahmann. 2012, November. Cyber warfare: Applying the principle of distinction in an interconnected space. *Israel Law Review* 45(3):381–399.

Gross, M. 2012. A declaration of cyber-war. *Vanity Fair*, April 2011. Retrieved May 12, 2012, from www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

Hagopian, A., A. Flaxman, T. Takaro, E. Shatari, A. Sahar, J. Rajaratnam, S. Becker, A. Levin-Rector, L. Galway, H. Al-Yasseri, J. Berq, W. Weiss, C. Murray, G. Burnham, and E. Mills. 2013, October 15. Mortality in Iraq associated with the 2003–2011 war and occupation: Findings from a national cluster sample survey by the University Collaborative Iraq Mortality Study. *PLoS Medicine* 10(10). http://www.plosmedicine.org/article/info%3Adoi%2F10.1371%2Fjournal.pmed.1001533. Accessed 9 Nov 2013.

Hashim, S., A. Ramli, F. Hashim, K. Samsudin, R. Abdulla, R. Azmir, L. Barakat, A. Osamah, I. Ahmed, and M. Al_Habshi. 2013, September. Scarecrow: Scalable malware reporting, detection, and analysis. *Journal of Convergence Information Technology* 8(14): 9–19.

International Committee of the Red Cross (ICRC). 2015. *Treaties and customary law*. http://www.icrc.org/en/war-and-law/treaties-customary-law. Accessed 11 Jan 2015.

Kaplan, D. 2011, October 18. New malware appears carrying Stuxnet code. *SC Magazine*. http://www.scmagazine.com/new-malware-appears-carrying-stuxnet-code/article/214707. Accessed 1 Aug 2012.

Kaurin, P. 2007. When less is more: expanding the combatant/noncombatant distinction. In *Rethinking the just war tradition*, ed. M. Brough., J. Lango and H. van der Linden, Chapter 6. New York: SUNY Press.

Kimmel, P., and C. Stout (eds.). 2006. *Collateral damage: The psychological consequences of America's war on terrorism*. Westport: Praeger.

Kinsella, H. 2011. *The image before the weapon: a critical history of the distinction between combatant and civilian*. Ithaca: Cornell University Press.

Pearce, M., S. Zeadally, and R. Hunt. 2013, February. Virtualization: Issues, security threats, and solutions. *ACM Computing Surveys* 45(2):17.

Raymond, D., G. Conti, T. Cross, and R. Fanelli. 2013. *A control measure framework to limit collateral damage and propagation of cyber weapons*. In: Proceedings of fifth international conference on cyber conflict, Tallinn, Estonia.

Rowe, N. 2013. Cyber perfidy. In *The Routledge handbook of war and ethics*, ed. F. Allhoff, N. Evans and A. Henschke, Chapter 29, 394–404. New York: Routledge.

Rowe, N. 2015. Distinctive ethical challenges of cyberweapons. In *The research handbook on cyber security*, ed. N. Tsagourias and R. Buchan, Chapter 14, 307–325. Cheltenham: Edward Elgar Publishing.

Shakarian, P., J. Shakarian, and A. Ruef. 2013. *Introduction to cyber-warfare: A multidisciplinary approach*. Amsterdam: Syngress.

Slay, J., and M. Miller. 2008. Lessons learned from the Maroochy water breach. In: *Critical infrastructure protection*, ed. E. Goetz and S. Shenoi, Chapter 6. New York: Springer.

Smith, T. 2002. The new law of war: Legitimizing hi-tech and infrastructural violence. *International Studies Quarterly* 46: 355–374.

TechRepublic. 2005. *Flaw finders go their own way.* http://www.techrepublic.com/forum/discussions/9-167221, dated January 26, 2005. Accessed 1 Aug 2012.

USCCU (United States Cyber Consequences Unit). 2009, August. *Overview by the US-CCU of the cyber campaign against Georgia in August of 2008*. US-CCU special report. http://www.usccu.org. Accessed 2 Nov 2009.

von Heinegg, W. 2012. *Neutrality in cyberspace*. In: Proceedings of the 4th international conference on cyber conflict, Tallinn, Estonia.

War Legacies Project. 2010. *Agent orange record*. http://www.agentorangerecord.com. Accessed 2 Mar 2015.

Neil C. Rowe is professor of computer science at the US Naval Postgraduate School where he has been since 1983. He has a PhD in computer science from Stanford University (1983). His main research interests are in data mining, digital forensics, modelling of deception and cyberwarfare.