Advanced Sciences and Technologies for Security Applications

Henry Prunckun *Editor*

Cyber Weaponry

Issues and Implications of Digital Arms

Springer

Advanced Sciences and Technologies for Security Applications

The series Advanced Sciences and Technologies for Security Applications comprises interdisciplinary research covering the theory, foundations and domain-specific topics pertaining to security. Publications within the series are peer-reviewed monographs and edited works in the areas of:

- biological and chemical threat recognition and detection (e.g., biosensors, aerosols, forensics)
- crisis and disaster management
- terrorism
- cyber security and secure information systems (e.g., encryption, optical and photonic systems)
- traditional and non-traditional security
- energy, food and resource security
- economic security and securitization (including associated infrastructures)
- transnational crime
- human security and health security
- social, political and psychological aspects of security
- recognition and identification (e.g., optical imaging, biometrics, authentication and verification)
- smart surveillance systems
- applications of theoretical frameworks and methodologies (e.g., grounded theory, complexity, network sciences, modelling and simulation)

Together, the high-quality contributions to this series provide a cross-disciplinary overview of forefront research endeavours aiming to make the world a safer place.

The editors encourage prospective authors to correspond with them in advance of submitting a manuscript. Submission of manuscripts should be made to the Editor-in-Chief or one of the Editors.

More information about this series at http://www.springer.com/series/5540

Henry Prunckun
Editor

Cyber Weaponry

Issues and Implications of Digital Arms

Springer

Editor
Henry Prunckun
Research Criminologist
Australian Graduate School Policing and Security
Sydney, Australia

ISSN 1613-5113 ISSN 2363-9466 (electronic)
Advanced Sciences and Technologies for Security Applications
ISBN 978-3-319-74106-2 ISBN 978-3-319-74107-9 (eBook)
https://doi.org/10.1007/978-3-319-74107-9

Library of Congress Control Number: 2018933519

Printed on acid-free paper

This Springer imprint is published by the registered company Springer International Publishing AG part of Springer Nature.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

For Orren

Foreword

The adaptation of digital technology is shaping to be the single most important influence on how human beings conduct their lives. In the twenty-first century, the cybersphere has created endless opportunities for the improvement of the human condition: how we feed and clothe ourselves, how we treat disease, poverty, and natural disasters. It has given us new ways to entertain ourselves and to explore happiness and the quality of life. Algorithms help fuel modern technological and scientific progress, both addressing the grand conceptual challenges and making our household appliances work more efficiently. Algorithms facilitate the delivery of critical services and in hundreds of other ways improve the quality of life. They do our banking for us even as they are opening our garage doors and monitoring our heart rates on bushwalks, all guided by the cyber-enabled GPS gadgets on our wrists. Importantly, cyberspace has helped democratize information, revolutionizing the way people receive and impart information and how they communicate between themselves.

At the same time, the cybersphere has created new vulnerabilities with potentially devastating impacts on our daily lives, our safety, and our well-being. Society is rapidly learning that cyberspace is providing a new vector for criminality and fraud affecting both great and small. It is already challenging traditional Western liberal notions of privacy. The so-called democratization of information can also mean the democratization of misinformation—accelerating confusion between objective facts and the conman's spin, making achieving the consensuses that democratic decision-making requires more difficult.

Conducting business over the Internet is having an impact on the way nation states approach their first responsibility: protecting the lives and safety of their citizens. In terms of national security, cyberspace has become the *fifth domain of warfare* after land, sea, air, and outer space. Warfare in the twenty-first century will be fought in cyberspace long before a kinetic shot is fired; it will inform and condition both actual armed conflict and its aftermath.

Warfare in cyberspace has three important facets: the collection of intelligence; the sabotage, disruption, or degradation of the opposition's cyber-dependent war-fighting capabilities (which can include not simply weaponry but also critical

infrastructure); and the ability to mislead and misinform through half-truths and concocted stories that are promulgated via social media. In short, the Internet, and our dependence upon it, offers a new vector through which to weaken an opponent's national resilience and war-fighting capability. Each of these facets has already been used by nation states, both in actual armed conflict and, alarmingly, in circumstances that fall short of armed warfare.

So, potentially damaging are the consequences of cyber-attack and so great the cost to nations having to fix the cyber vulnerabilities. We have allowed these shortcomings to open up because we have rushed pell-mell into cyber dependence. Societies and their governments now need to focus not simply upon repairing the damage, but on how innocent populations can be spared from the ravages of cyber-induced disasters, breakdowns, and damage, whether inflicted by nation states or non-state actors.

The response to cyber threats will be complicated, not least because prophylaxis inevitably lags the inventiveness of those who use the Internet to do harm. It will involve sophisticated technical solutions to protect our cyber-connected devices from infiltration and malicious activity; it will involve cultural or behavioral change in the way we respond to threats from cyberspace; it will involve legislation to force industry and cyber service providers to protect both privacy and the sustainability of the critical infrastructure which now depends on cyberspace. It will also require international cooperation to set norms and rules to govern both the offensive and defensive uses of cyber-technology, much as humankind has had to develop norms and rules to govern a range of transnational issues: the world's oceans, the natural environment, the use and proliferation of nuclear weapons, the management of contagious diseases, and how we address serious and organized crime.

The technological development of cyberspace and its rapidly expanding uses, together with mountains of data it generates, have become self-sustaining. This is not yet the case with the doctrines that ought to accompany the development of the Internet phenomenon. Our defense experts are still exploring the war-fighting capabilities developed for use in the cybersphere, as well as the technology and doctrines needed to defend ourselves against cyber-attack. We need to devote more intellectual effort to analyzing this technology's impact, the vulnerabilities it creates, and how best to mitigate the vulnerabilities. That intellectual effort must turn also to the ethical and moral dimensions and the obligations of the state to protect the privacy and the safety of its citizens against cyber-induced catastrophes.

With these critical issues in mind, I congratulate Dr. Henry Prunckun and his fellow contributors for their collaborative efforts in bringing together and analyzing so many strains of the cyber dilemma and, in doing so, making their arguments and research findings available to scholars, researchers, students, and policy-makers in such an easily read form.

David Irvine BA(Hons), AO
Chair, Foreign Investment Review Board (since 2017)
Director-General, Australian Security Intelligence Organisation (2009–2014)
Director-General, Australian Secret Intelligence Service (2003–2009)

Preface

Without a doubt, cyberspace has become *the* battlespace for confrontations. However, to conduct cyber operations, a new armory of weapons needs to be employed. No matter how many or how sophisticated an aggressor's kinetic weapons are, they are useless in cyberspace. This fact places, at least in theory, those with an inferior set of kinetic arms, or those without arms at all, on a footing that allows them to go head-to-head with all contenders.

So, contrary to popular opinion, the use of cyber weapons is not limited to nation states, though this is where news reports seem to focus. The reality is that there isn't a sector of the political economy that is immune to cyber-attacks. In this sense, an *attack* could be part of a limited cyber warfare, cyber espionage, or cybercrime. Some attacks read like Hollywood screenplays: "A group of hackers use a stolen cyber-weapon to try to extort money from people worldwide. The attack cripple [d] hospitals, causes ambulances to be diverted, and [surgical] operations to be canceled. Then, a lone security researcher stumbles across a way to halt the bug in its tracks. Yet, this is exactly what happened. . ."[1]

This book addresses the use of cyber weapons by national security agencies, the military, law enforcement, and the business sector—with the latter including those agencies termed *nongovernment organizations*. It looks at the milieu of the cyber weapons industry and the belligerents who use them; it also looks at what distinguishes these hardware devices and software programs from those that are used in general computing.

The text is divided into two sections, each examining a specific aspect of the topic—contextual issues of cyberspace in the new battleground, defensive cyber weapons, offensive cyber weapons, and dual-use weapons—and finally, it looks at the implications these weapons systems have for practice.

The book's concise chapters will appeal to scholars as well as students in the field because it incorporates practical case examples along with policy discussion. Course

[1] "The Worm that Turned," *The Economist*, May 20, 2017, p. 10.

instructors will find several learning aids that should be useful for lectures or student assignments. These learning aids will also be of interest for readers who are perusing professional development outside the classroom. To enhance these learnings, each chapter is accompanied by references to the subject literature. Where appropriate, the chapters are accompanied by tables or figures that illustrate points being made. Finally, there is a comprehensive index to help readers quickly locate the material.

I am optimistic that this text will find wide application, appealing to those in fields such as computing/information technology, national security/intelligence, military science, police/law enforcement science, political science, and law/criminal justice/criminology.

Sydney, Australia Henry Prunckun

About the Study Questions

Here is some advice about the study questions listed at the end of each chapter and how to approach and ultimately answer them:

Explain/list/describe: This type of question asks you to outline the factors associated with the issue under study.

Argue: This type of question asks you to present factors about the issue being investigated, but requires you to select one of the factors so that you can defend it.

Discuss: This type of question asks you to form a view (or judgment) after weighing up the for and against factors and then draw a conclusion(s).

Acknowledgment

The editor would like to thank the U.S. Department of Defense for the use of the visual information that appears in this book, but would like to point out that its appearance in this text does not imply, or constitute, the department's endorsement.

Contents

Chapter 1
Weaponization of Computers

Henry Prunckun

1.1 Weaponization

A prisoner sat on a locker-room bench drying herself after showering. She soon saw a group of prisoners approach and surround her. She looked around for the guard, but she was not in sight. Her heart raced; her breath became shallow. Despite no words having been spoken by those menacing her, she knew she was about to be given a beating.

If she was to survive, she needed help. But, with no one else to assist her, her only hope was for a weapon; something that would help equalize the odds. Nonetheless, being in a prison discounted this option—there were no guns, knives, or clubs. So, she reached for one of her socks, drop a bar of soap into it and swung it a circle over her head. She was now armed.

A device that is used to inflict harm on a person is considered a *weapon*, or *arm*. Arms are used to damage buildings, roads, and other forms of infrastructure. Weapons are used in a variety of positive ways, from helping to hunt for food, to humanly putting-down injured animals. But, arguably, the main purpose is to provide an effective means to harm an opponent. The effectiveness comes from the gain, or advantage, the weapon provides—in the case of our prisoner, it is in the potential delivery of the weight contained in the sock, and the mechanical advantage the leverage supplies, as well and the added speed of the delivery. A blow to the face or head will result in a greater degree of injury than the impact of a fist, and there is no pain or damage to the person delivering the blow.

Yet, a bar of soap and a sock are not weapons. However, they were weaponized—that is, they were combined to form a device that was a weapon. Depending on the circumstance and what is available, many everyday objects can be weaponized in

H. Prunckun (✉)
Australian Graduate School of Policing and Security, Charles Sturt University, Sydney, Australia
e-mail: hprunckun@csu.edu.au

H. Prunckun (ed.), *Cyber Weaponry*, Advanced Sciences and Technologies for Security Applications, https://doi.org/10.1007/978-3-319-74107-9_1

this way. Cars can be used to run-down people; pencils can be used as spikes to stab an opponent; drinking glasses can be used to lacerate attackers, and wine bottles filled with gasoline can be used to. . .

Chemicals, viruses, and radiological material can also be weaponized. History is littered with examples of chemical agents being used in war, and it is known that several countries hold stocks of biological weapons. At the time of writing eight countries[1] were conformed to have nuclear weapons—China, France, India, North Korea, Pakistan, the Russian Federation, the United Kingdom, and the United States. Radiological weapons are devices that are designed to spread radioactive material in densely populated areas. Acknowledged as less a hazard than a nuclear device, it is posited that this type of weapon has more psychological effect than physical harm—it is likely to be used to cause panic according to terrorist doctrine—"kill one, frighten ten-thousand." Nevertheless, there is plenty of sources of radiological material—it is held in places like dentists' offices, university laboratories, hospitals and clinics, and a person can make the equivalent of a Molotov cocktail with just a few components. Recall, it isn't the explosion that is the worry, it is the spread of the invisible radiological energy that will cause panic and economic injury. These weapons are referred to as *dirty bombs*.

This is all clear when dealing with the physical world—a person can visualize how they might go about arming themselves against attackers with an improvised weapon, but what about in the cybersphere? How does a person attack an opponent in the world of the Internet—a world constructed of optical fibre cables, routers, switches, ethernet cables, servers, and millions of computers? And, how does a person defend themselves in this world? A bar of soap and a sock just won't be enough.

1.2 Weaponizing Computers

Civilization occupies all the continents. All major islands are inhabited. The oceans and skies are populated with vessels and craft carrying people. Space is occupied by scientists aboard the International Space Station, and if today's visionary entrepreneurs are successful, space will have its tourists before too long. In all of these environments we can see examples of weaponization. We have taken motorized vehicles and mounted machine guns and cannon for offensive operations, and armoured plating for protection. We have done the same with aircraft and watercraft, and call them bombers, fighters, and warships. We have provided soldiers with rifles that once were used for hunting game, but the enhancements to these mean that they can now deliver a projectile hundreds of yards with precision; or in such rapid sequence that the number of rounds fired per minute sounds implausible.

[1] It is presumed that Israel has nuclear weapons, but this has not been established with any certainly.

A world exists in copper and optical fibre cables, magnetic disks and flash memory devices. Digital information that is created in this world by converting thoughts into representations through mechanical actions. These data are then stored on these devices. To communicate what has been created, it is transmitted via cables, and radio waves. But, is this really a *world?* Perhaps not, because the mechanical interface with the computer and the storage devices of a computer system exist in the physical world. So too do the apparatus that are used to transmit the electronic information—cables and the ether are in the physical world. Therefore, it is not really a world, but a metaphor that helps to conceptualize computer technology. Cyberspace is no more a world than books are a world. Yet, when we talk about "getting lost in the world of books," or "living in the cybersphere," we understand what is being implied.

If we accept the premise that information—ideas converted into digital representations—is the reason computer technology exist, then we can reason that the disruption of any process from mechanically entering the information (say, via a keyboard, mouse, e-pen, or voice command) to the reading, viewing, and/or listening to that information by the recipient, can form a target if the information is deemed to be a hazard. We can interdict and prosecute the two ends of this *kill chain*[2] without the weaponization of computers. We can, for example, arrest those involved with creating the information and receiving the information, and this will remove any risk this information presents. Take the case where a person concocts a plan to attack people at a busy city market. The planner transmits his plans over the Internet and are stored on a social media website. Others read it, and a conversation ensues; this dialogue culminates with four people carrying out the plan.

Arresting the planner would immediate remove the key to the illegal activity by denying the information on which the attack is founded. Arresting those reading the information would also achieve the same result. However, the laws of evidence, constitutional liberties, and the doctrine of due process could impinge on doing this, especially if the planner is domiciled in a country outside the target country, and those viewing the information are also in different countries.

Like transmitting information using radio waves, this information can be located (intercepted), and countermeasures that disrupt or destroy the data anywhere along the kill chain can be developed. After all, we are operating in the physical world—*cyberspace* is only a metaphor. This is done by taking what is normally used in electronic data processing and computer technology, and, like the fictional prisoner in our previous illustration, weaponizes these artefacts. The result is harm caused to the digitized information, and/or the means of creating, storing, using, or transmitting it.

[2]The term *kill chain* is used in the military. It refers to the attack process, or a *chain* of events and decisions. The process comprises: (1) identifying a target; (2) determining its location or position; (3) decision whether to attack; (4) and either standing-down, observing further, and/or using the data for intelligence, or to attack the target. Viewed in reverse, if an opposition's kill chain can be disrupted, the theory is that a successful attack is not possible.

1.3 How Is Weaponizing Done?

Clearly, there is no scope to use bars of soap and socks to improvise a weapon where computer technology is concerned. The digital world is characterized by electrical currents, wires, and tiny electronic components mounted on printed circuit boards. Sure, a person can hammer-away at a computer with an improvised soap-blackjack, but realistically, that isn't likely to result in a successful attack.

However, if an opponent's computer could be rendered inoperable without the need to be present, then the chances of success increase. This is done using the same infrastructure that processes and transmits information, only these "improvisations" are malicious.

Weaponization is done by two approaches—a software approach and a hardware approach. The first is by creating a program that when run, will perform an action that is not desired by the owner/operator. The terms *virus*, *worm*, *Trojan* are types of programs that are classified as *malware*—shorthand for malicious software. These can be standalone programs or parts of larger programs that allow the scribe to carry-out harmful tasks.

The hardware approach is where an electronic device is used to create harm. A keystroke logger is a type of device that is placed in-circuit with a computer and will record the mechanical input from the computer's keyboard. No elaboration is needed to understand the ramifications of doing this.

Consequently, like placing a bar of soap in a sock, when a person wires a simple recording device to a computer they have weaponised the device. When a software application is written to perform a destruction function, it has been weaponized. When a piece of software and hardware have been configured to operate in unison to act destructively, the system has been weaponized.

1.4 Who Does It?

Just as anyone can use a pencil as a spike, so too can anyone weaponized a computer. Who does this is best understood if these weapon developers are viewed on a spectrum. This spectrum could be described as the casual developer who creates a self-defence weapon because of genuine necessity—like the earlier prisoner example. At the other end of the spectrum are the world's global outlaws—societal malcontents who operate with psychopathic motives, or those who use simplistic philosophical arguments to justify their reasons.

There are also all those in between—those who are curious to see if they can do it (like a teenager who makes a zip-gun in his father's home workshop); those who are out for revenge (the employee who feels she was fired without cause); or to make a quick dollar (scammers and fraudsters); or those whose duty it is to protect society—law enforcement and intelligences agencies. Of course, there are more categories of weapon developers—

both defensive and offensive—but this list presents some idea of the range of people who engage in it.

1.5 Implications for Policy and Practice

1.5.1 Legislative Control

If anyone can "do it," it raises the question of who has these weapons. During the Cold War, the US and the Soviet Union kept close count of each other's nuclear weapons. Processes and procedures were put in place to verify what the each reported—some of these were covert intelligence gathering activities because the stakes were too high to not know what each side held in their arsenal.

On a smaller scale, domestic gun manufacturers are required to report the numbers and distribution of firearms; retail sales are recorded; and purchasers are registered. Although not perfect, authorities can estimate the numbers of guns in circulation. Though, on this point, the analogy ends. Although authorities know approximate numbers of guns in society, and their likely distribution—legal and illegal ownership—verification, in the sense of nuclear weapons, is not possible. And, this is an issue for policy and practice. As Prunckun questions in a later chapter; can society control these software programs through legislation, and should there be legal restrictions placed on the use of hardware devices? Enforcement might be an issue, but does that mean no controls at all? Governments face problems in policing firearms, but that doen't mean a repeal of all gun laws, which is, arguable, the case now with cyber weapons—a somewhat lawless situation?

1.5.2 Malware Marketplaces

Herr argues in his chapter that it isn't so much the payload of a cyber weapon that should be the central concern for policy-makers, but the factors surrounding the computer source code—making them reliable, accurate, and their distribution through malware markets. If the environment for their proliferation could be understood, then it follows that strategies for effective control can be devised.

If we look, again, at firearms, every school student understands how a firearm works; but what makes the device reliable and accurate, and how can these enhancements make a standard armament worthy of deployment against a target? This understanding is the information necessary to succeed as a weapons maker; whether it is a firearm or a cyber weapon. It is also necessary for regulators to know to be able to control these processes.

1.5.3 Need for Self-Defence

Although the cybersphere is a world analogous to a place created in the pages of a book—a virtual world—the interface between these electronic devices and software programs affects the physical world. Just as publishing a book has real-world affects—the ideas expressed in the words can result in action, or inaction—so too can the information in computer systems. After all, that is why information is put into these systems; to do something with it; to use that information to manage some aspect of society.

It is in this vein that a people would seek protect for their ideas and intellectual property—in whatever form that exists. Thomas, Low and Burmeister's chapter discusses how a Red Team-type exercise can provide computer users with information to protect their systems from criminals and state-based espionage. Known as *penetration testing*, this is a purposeful attack on an IT installation with software applications and hardware devices to test the system's robustness.

This approach is somewhat controversy because it could be said that possession of these programs and electronic devices are offensive weapons, even though they are being used defensively. Therefore, shouldn't policy take this into account? But, what about the integrity of the "pen" testers themselves? Should they be licensed to assure their personal integrity, and that they are able to control the applications they use and the devices they deploy? This is analogous to situations where law enforcement officers can use fully-automatic firearms, but the average citizen cannot.

1.5.4 Personal Privacy

Debate about Internet privacy has been argued in many forums for a long time. One side of the debate is that people using the Internet have a right to privacy. There is legal precedent for this in the Fourth Amendment to the US Constitution and under other legal traditions found in other jurisdiction's that are based on the philosophical principles found in the theory of natural rights.

Regardless, a person's right to privacy is not absolute. The test as to whether a person has an expectation to privacy is based on what is observable by the five senses in, or from, a public place—the plain view doctrine. A right to privacy is also abolished when a court issues a law enforcement agency with a search warrant, or a law enforcement officer exercises a legal power to conduct search without a warrant.

This raises the question as to whether everything done on the Internet is private? Blog posts can be seen in the same way pinning a notice to a public bulletin inboard can. So, should online shopping be considered the same as shopping in a mall or department store? Can browsing various websites for a summer vacation destination,

or anything else, be considered the same as window-shopping? When these activities are carried-out in the physical world, they are conducted in public view; so, can the same public observation be an expectation when viewing goods and services on the Internet?

No doubt the courts will wrestle with this issue for some time, but what about the issue of a person installing a key-logger into a USB port of someone else's computer? This may overstep the bounds and not only be a breach of privacy, but constitute criminal thief (or a civil wrong for breach of contract if done in a business settling), and depending on the target, espionage. In the meantime, how does a person, business, NGO, or government department ensure privacy until courts provide clearer definitions of what is and isn't private? Irwin's chapter looks at how common computer security techniques and methods can be used to help overcome cyber-criminal activity.

1.5.5 Dual-Purpose Weapons

Dealing with cyber-criminal activity with some of the time-honored computer security approaches is fine, but these software programs and electronic devices can also be used by the same criminals they are meant to protect against. Referred to as dual-purpose weapons, they can be both defensive and offensive. Several chapters in this book touch on this issue. Like other cyber weapons issues, there is no clear answer as to how it is addressed because much of the problem lays in the mind of the person who is using the program or hardware—in legal circles this is known as *intent*.

Take as an example a person who buys a second-hand mainframe computer. She sets it up in her garage with her other computer and networking equipment. But, rather than using it to help her solve mathematical problems related to astrophysics, she uses it to solve password encryption problems related to a classified government database. Having a mainframe computer is not a problem, but weaponizing it in this way is.

1.5.6 Business Sector and Non-government Organizations

Self-protection also extends to the business sector and to non-government organizations. McGonagle and Whitford in their respective chapters discuss how commercial-in-confidence information requires the highest levels of protecting to ensure the viability of free-market economies. Likewise, organizations operating to provide aid and social-relief, and issue motivated groups aimed at bringing about