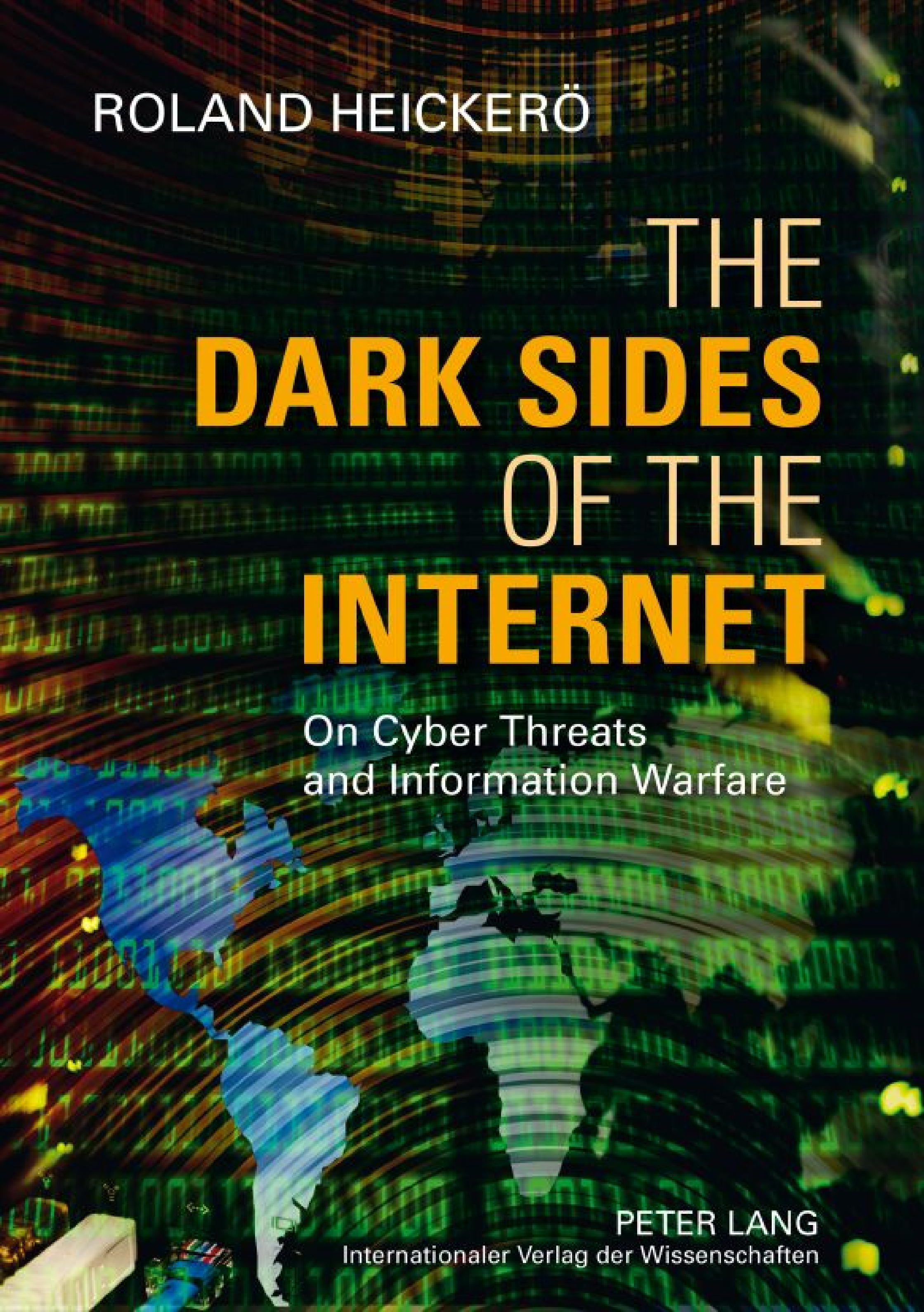

ROLAND HEICKERÖ

THE DARK SIDES OF THE INTERNET

On Cyber Threats and Information Warfare

PETER LANG
Internationaler Verlag der Wissenschaften

The Dark Sides of the Internet

ROLAND HEICKERÖ

THE DARK SIDES OF THE INTERNET

On Cyber Threats and Information Warfare

PETER LANG
Frankfurt am Main · Berlin · Bern · Bruxelles · New York · Oxford · Wien

Bibliographic Information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the internet at http://dnb.d-nb.de.

Cover and Photo Design:
© Olaf Glöckler, Atelier Platen, Friedberg

Translated from the Swedish original
Internets mörka sidor.Om cyberhot
och informationskrigföring,
published by Atlantis Bokförlag, 2012.

Translated by Martin Peterson.

ISBN 978-3-631-62478-4 (Print)
ISBN 978-3-653-02502-6 (E-Book)
DOI 10.3726/978-3-653-02502-6

www.peterlang.de

Table of Contents

Preface

Years ago, when I worked in the telecom sector for the wireless operator Telia Mobile and later on for Ericsson, I became interested in the mega change we are into to today – the information revolution. At that time mobile phones and the Internet were relatively new phenomena. As more and more people are getting connected to the global network and use more advanced services and applications, questions arise regarding how to secure and protect information, and information and communications systems.

From having developed mobile systems, I now try to understand vulnerabilities and security holes in networks and functions for illigetimate cyber activities and their eventual consequenses at security policy level as well as at socio-technical systems levels. This book tries to explain the growth of varied and serious phenomena on the net, the dark sides of the Internet, including the battle for information superiority, cyber terrorism, criminality and espionage as well political-ideological hacking, “hacktivism”.

For fruitful discussions on different aspects of information security and cyber threats, I would like to thank my friend and co-worker Dan Larsson, senior expert at the Swedish Defence Radio Establishment. I also want to express my gratitude to “Nico” and his colleagues at the Swedish Armed Forces for their profound knowledge and stringency within the field. Lars Nicander, head of the Center for Asymmetrical Threats and Terrorism Studies (CATS) at the Swedish National Defence College, deserves great praise for his expertise and his neverending will to convey insights and knowledge on this important subject.

A also want to give my thanks to my former collegues at the Swedish Defence Research Agency, especially John Rydkvist, Jerker Hellström and Alexander Atarodi.

This book is dedicated to Anna, Vilgot, Hanna and Moa.

Stockholm, September 2012

Introduction

Terms like cyber threats, information warfare and digital attacks are charged to many people, surrounded by an aura of mysticism and secrecy. This is quite natural. The phenomena are relatively new. They are a result of the information revolution, which in its turn can be experienced as complex, difficult to interpret and multidimensional. It is also a field surrounded by a high level of secrecy, since it involves different kinds of illicit influences on information and information systems – and protection against such activities.

The first time the word "cyber space" was mentioned in more broad terms was in the 1984 novel *Neuromancer* by science fiction writer William Gibson. It has become very popular and is used in a number of different contexts to describe the virtual world of online computers and networks and what is in between in the form of data flows and interacting users.

Pioneering technological breakthroughs such as the Internet, mobile phones and computers have resulted in radical changes in people's possibilities to communicate and spread information as well as handle electronic transactions of different kinds. These innovations are just as important and decisive to humanity as Gutenberg's printer in his days. They fundamentally affect societal structures and give rise to new logics and business models. The Internet makes it possible for users to gather, store, process and send large amounts of data. It is a force that makes globalisation possible. The Internet breaks up information monopolies and opens up for competition about the scope in cyber space.

Access to distribution channels such as TV, radio and newspapers are no longer as vital as they have been to spread messages and influence public opinion. Via blogs, web sites and Internet forums practically anybody can make his or her voice heard. This changes power conditions. Increased opportunities to communicate and spread information also means that new technology and new methods, which previously were difficult to provide or too expensive and complex, can be used by more and more people.

The use of communications technology penetrates all levels of society. In high-technological societies it can be difficult to defend oneself against the wave of data that flows from apps, cell phones and computers, and which often demands that the user is available immediately. A lot of the information that is spread can be perceived as relatively uninteresting, other parts as important and valuable. It can lead to increased understanding and a better grasp of various phenomena. Attitudes and outlooks change. In the long run this can lead to increased democratisation and new knowledge.

Non-democratic regimes hardly see the development as positive, but rather as a threat. The powers that be try different methods, such as censorship and supervision of users, to prevent information from being spread. They obstruct the conditions to create meeting places – communities – on the web where knowledge and experiences can be conveyed. The capacity to process and convert data into information and simply and cheaply send it to third parties sets powerful forces in motion. In extreme cases it can manifest itself in popular protests against abuse of power such as in North Africa and the Middle East in the spring of 2011 and in Iran in 2009.

The global number of users with access to the Internet is more than two billion. Every month the web grows by tens of millions of new users. Since its commercial breakthrough in the mid-1990s the Internet has developed into an enormous meeting place and linking force. Cyber space can be defined as multi-polar in the sense that it consists of a countless number of players from all the corners of the world. Using different kinds of information and communications services has become part of everyday life in all modern societies and most people can now hardly imagine life without them. Social media such as Twitter and Facebook are used to connect people. Phenomena such as Wikileaks, Wikipedia and YouTube would not exist without the global web.

While information technology has a number of positive results for most people, harmful conducts and activities have also evolved parallel to these. The conditions for antagonistic conduct have changed. New threats are created as cyber space expands. This kind of aggression cuts through the whole societal spectrum and affects both civilian and military structures, governments, organisations and companies as well as the individual citizen. The reason for this is partly society's major dependence on information technology, partly that the systems are so intimately intertwined. Cyber attacks against the electrical grid, for example, can have an effect on telephone and computer networks. This in its turn risks having dispersion effects in other sectors and businesses such as financial systems, aviation and so on. The result is serious disruptions of infrastructure that is vital to society.

Information warfare

Information warfare can be used at strategic political-economic level in diplomatic talks between parties during negotiations or as an economic means of bringing pressure to bear on another nation. It can also be used at tactical and operational level close to or in connection with a military conflict.

However, information warfare is in itself not in any way limited to states' actions and relations between nations, but covers the whole range of human activities and conducts. In the original sense it is referred to the individual and takes place in interaction between people and organisations. This has been going on for as long as humans have existed. The purpose is to make opponents act in a way that is advantageous to oneself. Human perception can be manipulated in subtle ways at which the subject's opportunity to correctly interpret the situation is rendered more difficult. This can either be done directly against the opponent, eye to eye, or indirectly via different kinds of technical systems and means.

Access to information and the ability to use it to one's own advantage are intimately related to power and control. On the analogy of this, the lack of relevant information or access to inaccurate information results in an incapacity to make correct decisions, which may be decisive and, depending on the context, lead to serious consequences. This applies generally, irrespective of whether it involves a person who is going to perform a single transaction, a company which is going to make an investment decision or a great power that bases its strength on information superiority.

Information warfare is a comprehensive collective term which includes different parts of the electromagnetic spectrum such as radio, radar, laser and electromagnetic pulse weapons. Other activities that belong to this category are psychological operations, military deception and computer and network operations. The latter are usually designated cyber warfare on the Internet. Included in information warfare are also different aspects of protection of information and systems.

Computer and network operations are asymmetric in character. From a relatively minor stake, the effect can be very big. A digital attack against a system requires fairly small resources, while it is costly to defend oneself. That way, the barriers are lowered for this kind of attack.

Using modern information technology, the distance to the target is not necessarily a problem. Cyber threats can arise anywhere in the world and knock out not only computers but cell phones and other units that communicate over the Internet. In some cases it is difficult to know who the actual instigator behind an operation is. The same can also be true of the target and the purpose of it. The web makes anonymity possible. Intentions can be hidden in the cyber fog.

At the same time, anonymity means that there is a risk that the wrong culprit is singled out and that defence measures against an attack are disproportionate – that the defending party resorts to more advanced cyber weapons against the party that is believed to have initiated the attack. That way, there is a risk that a conflict escalates very quickly.

Examples of targets are individual states, but also companies and organisations, groups and individuals. Harmful cyber activities can involve spreading propaganda or misleading information, industrial espionage or aim at tapping, interrupting or destroying information, computers and networks. The opponent can also have his access to vital and sensitive information blocked and thus be prevented from acting.

The Internet is in itself a very useful channel for distortion through rumours and slander conveyed *en masse* via social media and networks. Anyone exposed to this will find it very difficult to defend him- or herself. Just as the Internet is a channel for dissemination of information, it can be used for repressive purposes by less scrupulous regimes and organisations in order to survey the activities and conduct of their critics on the web. By e.g. planting malicious code, such as viruses, worms and trojans, infringements and hacking as well as denial-of-service attacks against important systems, an opponent's desire and capacity to defend himself can be reduced.

In cyber space there are no clear boundaries between military and civilian infrastructure; they are integrated and interdependent, since they often share the same communications networks. As long as nations depend on computer networks for their basic economic and military power, and as long as these can be accessed from the outside and the inside by people with bad intentions, there are thus risks.

An advanced cyber attack directed against an opponent's vital information infrastructure – especially command and control functions in electricity, telecommunications and computer systems, financial institutions, the energy sector, air traffic etc. – can have serious social and security political effects in a short time. Important and vital functions may be discontinued permanently or over a limited period of time. This means great challenges to the responsible parties.

The first officially published cyber attack on an individual state was carried out against Estonia in the spring of 2007. In connection with the transfer of a Soviet military statue from central Tallinn to a cemetery nearby in the city, a number of cyber attacks were initiated against computer systems in the Estonian parliament and several ministries, two of the biggest banks and six news organisations and various other national web sites. In a few days servers and networks were overloaded, at which functionality went down. Who or what groups and organisations were behind this attack has not been made clear. But suspicions have been pointed at Russian nationalist hacker groups – so-called hacktivists. The attacks ceased as quickly as they began.

In a 2003 intelligence report on cyber defence by the U.S. Navy the following estimate was done: A group of some thirty hackers, strategically located and with a budget of less than 10 million U.S. dollars, could shut down large parts of the critical infrastructure in the United States in a well co-ordinated attack.[1]

A computer found by U.S. forces in one of al-Qaeda's buildings in Kabul contained a model of a virtual dam.[2] Apart from the model there was a programme that simulated what effects there would be on people and equipment if the dam broke. The direction and propagation of the water masses could be calculated. The example shows that al-Qaeda's activists are well versed in the use of computers during tactical planning of operations.

[1] Atwan, A.B. (2006) "The Secret History of al Qaeda". *University of California Press*. Berkeley, USA.

[2] Borger, J. (2002) "US fears al Qaida hackers will hit vital computer networks". *The Guardian*, 28 June 2002.

Cyber aggression

Cyber warfare is something that is pursued by many kinds of players. Behind an operation there may be a resourceful national intelligence and security service as well as an organisation without national ties and which acts independently and idealistically. An operation can also be carried out by a small group of dedicated hackers with good IT skills, by criminal organisations, by insiders and terrorists. Unholy alliances can arise between different kinds of players. For example, a state can use cyber crime groups as tools to attack another state.

For the great powers, cyber space is an area of battle and protection. It is a question of defending the country's sovereignty in the digital sphere. Cyber weapons can be used as an individual resource against an enemy or in combination with conventional weapons systems such as aircraft, tanks, missiles and weapons of mass destruction. It changes the balance of power between opponents, since a party that is militarily weaker on paper can gain strategic, operational and tactical advantages in cyber space against a seemingly stronger rival. This makes cyber warfare attractive.

Planting malicious code such as the *Stuxnet* worm, which was discovered in June 2010, is an example of this new phase of warfare.[3] The malicious code was tailor-made to attack master computers at the Iranian uranium enrichment facility in Natanz. Through Stuxnet, centrifuges that were used for enrichment could be inaccurately adjusted which resulted in a number of them being subjected to abnormal wear and destroyed. In different contexts Israel and the United States have been singled out as the instigators of the operation. In 2012 an even more advanced malware was discovered known as *Flame* or *Skywiper* addressed to attack computers running Microsoft Windows. It targeted computers in the Middle East, especially in Iran, and some sources claim that Israeli computer experts were behind it. In the autumn of 2012 another malware, *Gauss*, was discovered – it is similar to Flame and designed to hit banks in the Middle East. The virus is said to come from the same "factory" as Stuxnet. Other examples of events that can be described as cyber warfare include Chinese hacker groups that have broken in to the Pentagon's computer systems in order to steal sensitive information.

[3] Beaumont, C. (2010) "Stuxnet virus: worm could be aimed at high-profile Iranian targets". *The Telegraph*, 23 September, 2010.

Today all technologically advanced states are developing concepts for network and computer operations. Doctrines are rewritten and adjusted to altered demands and new threats. The great powers are setting up organisations in order to defend their own information resources and communications systems and be able to spy on and strike against hostile ones. In October 2010 the *U.S. Cyber Command*, specialised in digital warfare, became operational. The organisation is led by the chief of the strategic signals intelligence organisation, the NSA.[4] As of this, cyber warfare has been ranked in the same category as the other strategic functions for the army, navy, marine corps and air force.

In a similar way Russia and China are building up their capacity, resources and units for digital warfare under the command of their military organisations and intelligence and security ministries. NATO, in its strategic doctrine for 2010, specifically pointed out cyber warfare as one of the most serious threats to the alliance and the countries that are part of it.

Western European countries are in no way exempt from antagonistic activities that can be suspected of having links to foreign powers. Foreign hacker groups have made attempts to penetrate objects of vital importance to society. High-technological activities are very much exposed to cyber espionage. This is especially serious for a country that builds its economic base on innovations. Cyber crime directed against companies and individuals is a growing problem, with huge sums in yearly turnover.

Terrorism over the Internet, where web pages and other means of communication are used for spreading messages and radicalising people, has been performed by European citizens. One conspicuous example is the case of the Swedish suicide bomber Taimour Abdulwahab in Stockholm a couple of days before Christmas 2010. In the wake of the attacks by Islamist Mohamed Merah in Toulouse in March 2012, French authorities have talked of banning its nationals from visiting web pages on the Internet that harbour radicalising messages.

Structure and contents

The cyber attack against Estonia in the spring of 2007, when a number of servers and networks were overloaded, shows the possible effects and conse-

[4] NSA – The National Security Agency.

quences of a computer and network operation. The case has become something of an alarm bell when it comes to the risks of attacks against vital communications infrastructure. The great powers building up their cyber warfare capacity, the Stuxnet worm and hacker operations in order to steal information reflect the same reality. Added to this there are various kinds of illegitimate and criminal activities.

Every modern state thus has to create strategies and courses of action in order to protect information, networks and computers that are vital to society from malicious cyber activities. Creating secure systems and minimising risks of information being leaked or tampered with should be a prioritised task. It is also important to understand what threats arise from the information revolution.

The purpose of this book is to give a broad background to the development of the dark side of the Internet and its consequences. It is not about scaremongering, but about creating understanding and knowledge and thus preparedness in order to handle detrimental activities. It describes the change in progress and what it may mean to society, companies and individuals as well as to military and police activities. Important issues such as integrity and censorship and the like are not specifically discussed in the text, only in general terms. Nor can every aspect of information security be described.

The first chapter of the book initially describes different kinds of players and antagonists with malevolent behaviour on the Internet. This is followed by a discussion on the methods used for detrimental activities via computer and network operations. The text gives a general background to the coming chapters in the book, where the player categories and different phenomena are discussed in more detail.

The second chapter of the book deals with the American, Russian and Chinese view on information warfare, which has been described in different doctrines and by leading military theorists and analysts. There is a historical background from the 1970s and onwards as to how different concepts and theories have developed from command warfare and network centric logic to information operations and cyber warfare.

Cyber terrorism is a phenomenon that is gaining more and more attention. One reason is the concern that modern information and communications technology may be used in order to harm open societies. This concern also involves actual IT systems and the information generated being targets of advanced attacks. That way functions that are important to society could be affected. The term cyber terrorism is complex. The third chapter of the book describes the difference between traditional and cyber terrorism. The main focus is on how the al-Qaeda terrorist network acts in cyber space, and on al-Qaeda's change in concentration and activities into a clever player in an electronic Jihad.

One of the most serious threats to a modern country's trade, industry and long-term economic development is industrial espionage and insiders. The activities are directed against high-technological industries and companies with advanced basic research. The defence and telecoms sectors are of particular interest, just as biotechnics, medical and material technology. Behind this kind of espionage there may be individual states and security services as well as competing companies. One trend is that criminal players are getting involved both as thieves and fences of information. Computerisation and the development of the Internet drastically increase the possibility of procuring sensitive information through illegal means. This can be done in different ways. In the fourth chapter there is a background. A number of examples are provided of how industrial espionage has been revealed and of the methods used during collection of information over the Internet – such as signals intelligence, monitoring of traffic, penetration and overtaking of computers with the aid of trojans. The chapter ends with a discussion of the Chinese cyber espionage network GhostNet which was discovered in 2009.

Criminality over the Internet is a growing problem. Globally, huge sums are being turned over every year. The fifth chapter of the book describes the development of small-scale digital criminality in the early 1970s to the present advanced, large-scale and cross-border operations. Examples are provided of the actions of criminal groups and hackers on the dark side of the Internet in order to steal information and commit fraud. The chapter also describes the black market for stolen information, which is traded and sold on secret servers. A lot of the crimes can be related to areas with a lot of corruption in combination with weak legislation in defence of private property. Quite a lot of cyber criminality derives from Eastern Europe, South East Asia and parts of Africa, particularly Russia, China and Nigeria. American cyber crime is also discussed; some of the world's most notorious hackers are from North America.

Hacktivism – or politically, religiously, ethnically and ideologically motivated hacking of opponents' networks and servers – is a growing problem. The sixth chapter provides several examples of hacktivism that have led to confrontations between groups of hackers and where the origin lies in political, religious, national and ideological differences of opinion. The text dis-