In recent years, the image of “the Internet” in political discussions shifted from ideas of an exciting new world to a potentially dangerous place. In the aftermath of 9/11, a new threat emerged out of vague ideas of cyber terrorism: cyber war. In this paper, I will map potential definitions of cyber crime and cyber war. I will sketch them on a theoretical level as well as give technical background information. Finally, I will argue that both phenomena—cyber crime and cyber war—are not well-definable and thus not precisely distinguishable. As it turns out, discourses on cyber war tend to militarize those on cyber crime—making their difference even more vague.

What is cyber war? Trying a definition by genus and differentia, cyber war is a distinct kind of war. War is in a common sense definition taken from a dictionary “a state of open, armed, often prolonged conflict carried on between nations, states, or parties” (The Free Dictionary) or “a state of usually open and declared armed hostile conflict between states or nations” (Merriam Webster). “cyber” on its part is an attribute meaning “of, relating to, or involving computers or computer networks” (Merriam Webster). Putting this together, cyber war is a state of usually open, armed hostile conflict between nations, states, or parties which is relating to or involving computers or computer networks. It is clear that every modern contemporary army uses computer technology in some way. Hence, every war nowadays could be regarded as a “cyber war.” Therefore, one should not speak of “cyber war” but of “cyber warfare” to emphasize the computer related aspects of war without suggesting a new distinct kind of war itself.

However, it has been suggested to think of “cyber war” in both ways: as a new aspect of war and as a new kind of war. Examples for such wars could include the attacks in Estonia in 2007 and the STUXNET worm in 2010. But as I will argue, there is no way to decide, if these incidents can really be regarded as cases of “cyber war”. Nevertheless, the term “cyber war” is used in literature and in political discussions. So, while it is hard to tell, if those example can be regarded as instances of cyber war, it is clear that there is indeed a cyber war discourse.

The same question is to be posed on the second phenomenon: what is cyber crime? Trying a definition by genus and differentia again, cyber crime is a distinct form of crime. Again taken from dictionaries, crime is “an act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction” (The Free Dictionary) or “an act or the commission of an act that is forbidden or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment my that law” (Merriam Webster). Unlike modern warfare, we can indeed imagine crimes without computers. Just think of shoplifting, fraud, or homicide. However, when it comes to international organized crime or white collar crimes we can hardly imagine the absence of modern technology. In fact, drug traffickers, for example, use modern automatic, i.e. computer controlled, submarines to cross the Mediterranean Sea. Furthermore, on platforms like eBay or with electronic cash systems organized crime has found new areas. Obviously, there is indeed something

---

1 Cf. Gaycken 2010, pp. 169-180, for more examples.
2 One can find many recent discussions, e.g. the new NATO strategy, the German “Cyberabwehrzentrum” or America’s cyber security plans.
like cyber crimes. However, their relevance is still controversial and subject to harsh political discourses—at least in most Western countries.

With these ideas on cyber war and crime, I want to try mapping both by showing some problems in distinguishing them. In the definitions I discussed above, a difference can be drawn between different actors: with war we find states, nations, and parties as actors. In fact, this definition neglected the role of combatants who are juridification of soldiers to distinguish them from civilians. Particular acts of war are executed by combatants. Therefore, a definition distinguishing between acts performed by states, nations, or parties and those performed by individuals does not work. However, a definition concerning different roles of individuals seems to work: acts of war are done by combatants in a conflict, criminal acts by civilians. Unfortunately, the first part of this try is circular. To define some individual as a combatant, there must already be a declared war and this is just part of the problem I am investigating. Hence, a definition working on individuals that are identified as combatants in the realm of public international law or as criminal offenders in the realm of national criminal codes does not work either.\(^3\) We can retry to reshape definitions concerning the sides of acts, their targets, their means, their intensities, but it will all boil down to the question: who performs the act? And then, is this particular actor a criminal offender or a legitimate combatant?

Imagine, we have solved this problem and identified the actor. By having identified him, I want to imply that we are able to answer certain questions about the actor. For example: is the the offender/attacker (\(o\)) and his or hers doing state-supported (s) or is she or he autonomous (a)? Then we could easily conclude:

- If (s), then (\(o\)) can be regarded as a combatant,\(^4\) it is an act of war.
- If (a) and the state, where the actor is, tolerates the act, it is an act of war.\(^5\)
- If (a) and the state, where the actor is, fights the act, it is a criminal act.

Of course, one can think of other approaches, e.g. analyses of “cui bono” or of the intensity of the attack. However, it is neither necessarily obvious who benefits from an attack, nor were a line between different intensities can be drawn. Just try to compare the intensity of an extremely successful act of crime versus a failed belligerent act.

In this very rough scheme of definitions, we find the problem of attribution repeatedly. Without attribution, it is impossible to identify an attacker and hence to decide if an incident is an criminal act or an act of war. The existence of this problem is common sense in current discussions on “cyber war” (cf. Gaycken 2010). Below, I will discuss in detail, why attribution is an unsolvable problem.

Take the ius ad bellum for example. Chapter VII of the UN charter grants the members of the UN the right to defend themselves against foreign attacks. However, the chapter emphasizes the role of the Security Council which has to “determine the existence of any threat to […] peace”. (Article 39) At the same time, every defensive act in a war has to fulfill certain [parameters]: since these act are violent acts, their targets have to be just participants of war (i.e. combatants) and so on.

So, we do not have a well-definition of cyber war since we cannot solve the problem of attribution.

---

\(^3\) While crimes are to be defined through criminal codes (nulla poena sine lege), we are used to think of war as acts that are belligerent de facto, not de jure.

\(^4\) Of course, I neglect some details here.

\(^5\) This conclusion is, of course, rather problematic. It shows the failure of attempts to build a international legal framework for warfare. I regard this conclusion to be true de facto, since phenomena like informal combatants or asymmetric warfare have replaced the idea of an declared, open state of war—if there has ever been such a thing in the first place.
However, we can think of preliminary definitions that include considerations of necessarily vague parameters like the already mentioned “cui bono.” Still, we can find an example which crosses the borders between crime and war in every case.

Let us put this musing aside for a moment and consider the technical cyber threats that are sketched in contemporary literature on “cyberwar.” Here, different targets and means for attacking are discussed. Let me first discuss targets, then means.

Possible targets of attack include, but are not limited to: communication infrastructures like telephone and data networks (e.g. the Internet); critical infrastructures through traffic control systems, power systems, and water supply systems; the financial system; the health care system. Last but not least, many armies have integrated highly sophisticated, but still technically insecure computer systems in crucial parts of their command infrastructure. Since they keep using off-the-shelf technology (Cf. Gaycken, Sandro: Cyberwar, 2010, p. 75), they have become an attractive target for hostile forces. Let me give you some technical background information on possible targets: for instance water supply systems, the financial systems, and communication infrastructures.

Water Supply Systems: Modern versions of those systems are controlled by SCADA systems. These control pumps and turbines. An attacker who manages to gain control of a SCADA system could reprogram it to start and stop turbines in an unusual high frequency. This would cause vibrations that would destroy the turbines. (It is said that STUXNET worked this way. However, STUXNET attacked, as far as I know, uranium enrichment centrifuges in Iran.)

Financial Systems: A few months ago, one could read about an attack on emissions trading. Hackers had sent phishing e-mails to gain access to account from which they transferred emission certificates to sell them. An attacker could generate a profit by skillfully combining stock trading, tapping access codes and obstructing competitors. Especially in this case we can imagine the problem of telling crime from war: Destroying major parts of a country’s economy is certainly an act of war, but what if a minor criminal attack gets out of control?

While some targets as the water supply system are targets for warfare and terrorism exclusively. But as the example of the financial systems shows, many targets can not be assigned to either war or crime. Even an attack on such a basic system as the SSL-PKI shows this ambivalence: Breaking cryptography allows to industrial espionage as well as surveillance of dissidents.

Means for attacking these targets include, but are not limited to: computer viruses and malware of any kind—including software and hardware, exploit codes, software and hardware bugging devices, and social engineering. Let me again give some technical background information, for instance: computer viruses, exploit codes, and social engineering.

Computer Viruses: viruses and other kinds of malware are programs that copy themselves through computer networks and digital media. Some programs manage to spread by deceiving users. The purpose of all malware is to manipulate processes, to tap data, to destroy software, sometimes also hardware—in the interest of their programmers.

Exploit Codes: These are codes that exploit vulnerabilities in software to circumvent security barriers.

---

7 I cannot point out the meaning of this infrastructure for any kind of cyber attack in detail here. Just remember the attack on the certificate issuer Comodo in March 2011. In this incident, allegedly a single Iranian hacker managed to tap access codes for Comodo’s security infrastructure and created certificates for the websites of Yahoo, Skype, Mozilla and Google. With this, it is possible to hijack a presumably secure connection and to inject malware into webbrowsers. Cf. http://www.h-online.com/security/news/item/SSL-meltdown-a-cyber-war-attack-1214104.html.
for examples. An exploit code is in some sense an information on security holes that are triggered by programming errors. Therefore, they can be used to close the holes as well as for exploiting them. In consequence, they can be used as a commodity. Today, one could buy ready-made exploit codes for security vulnerabilities that have not been revealed to the public yet. At the same time, intelligence agencies use to search for vulnerabilities and to collect appropriate exploit codes as some kind of weapon in the cyber war to come. Ironically, if they revealed this information to the software companies, no-one could use the code anymore after a short time period.

**Social Engineering:** A third kind of means in a cyber attack is social engineering. Here, an attacker deceives persons who already have access to the system that is to be attacked. A simple, but famous example is the attacker who calls the staff, introduces himself as an engineering working at a remote site on a very urgent problem and desperately asks for a code printed on a device right behind the desk.

While counter measures to all these means are possible, it is common sense among computer scientists and security researchers, that it is not possible to build a “secure computer system.” One could get nothing but a more or less secure system.

With this technical background in mind, let me say something about the reason for attribution being an unsolvable problem. As I pointed out, the problem of attribution is to attribute every act an actor, be it an individual, be it a distinct organization. In the case of cyber attacks, attribution means to identify the attacker. To cut a long story short, consider attacks performed on the “Internet”, that means on a heterogeneous, global computer communication networks that uses TCP/IP as its standard protocol.

Let me first give an example where attribution is possible. Think in comparison of nuclear attacks. Granted that no act of deceiving takes place, it is possible to attribute a fingerprint of radioactive isotopes scattered by a nuclear bomb to a certain reactor in the case of Plutonium or to a certain mining area in the case of Uranium. By this, one could attribute a surprising nuclear attack ex post to a certain attacker as long as the isotope fingerprint is known. Although necessary data is top secret and the math is not trivial, attribution can be solved with nuclear weapons in principle.

Contrastingly, with digital communication there are no fingerprints that can not be counterfeited. A connection on the Internet is defined by two IP addresses and two TCP port numbers. One address and one port for the sender and one such pair for the receiver. Since the numbers used for these change over time for reasons I cannot point out here, it is necessary to include timestamps for describing connections. Internet Service Providers (ISPs) can attribute connection to their customers. So in theory, it is possible to attribute connections to certain users, with data retention even ex post. In reality however, it is possible for attackers to counterfeit connections, to use compromised computers and routers as proxies etc. By that, attackers can cover up their tracks. In fact, this is quite easy due to the (by law) heterogeneous, international structure of the Internet. And even if one manage to track such a covered connection, one could end up on a computer without knowing if this machine was the original source of the attack. An attacker could misguide by using proxies in usually suspected countries like Russia or China. Of course, this does not tell anything about the original source of the attack, since it is plausible to cover up by blaming others.

---

8. Among other data, it is this information that is collected in the European Data Retention Directive. Without this Directive, ISPs are, for example in Germany, not allowed to store this data due to data protection laws. The directive has been ruled to be unconstitutional in some countries, e.g. in Germany and in Romania.

9. This is the reason for data retention not to work with transnational organized crime. It works, however, with unprofessional offenders who lack the technological knowledge to cover up their tracks—with an huge impact on the society, though.
The fact that it did not introduces means and targets of cyber attacks without sharply distinguishing war and crime in the first place, is neither carelessness nor a trick to support my argument. As a matter of fact, cyber crime and cyber war mix with regard to means and targets in many cases. And even if we manage to clearly tell war from crime in some cases, we will find a large gray zone. However, neither is this gray zone specific to cyber attacks, nor are there no distinguishable—white and black—extremes in this area. For example, with conventional warfare and crime, many means mix, too. Just think of the machine gun which spread from the army, to so-called terrorists and to organized crime. And there are indeed means and acts that can be assigned to crime and war: shoplifting is by law a crime, but seldom an act of war. Nuclear bombs are seldom used even in organized crime. However, one cannot find such differences within the means of cyber attacks: vulnerabilities in program code are pretty much the same in both cases. The STUXNET worm, for example, used, inter alia, a problem in the printing system of Windows XP on local networks and a flaw in Windows' code for processing certain file for spreading through thumb drives. Of course, printer and thumb drives are common technology and can be found within virtually every computer nowadays.

Above, I suggested to distinguish ordinary war and ordinary crime by the different law codes defining them. I argued that this solution could not be applied on cyber war and cyber crime. It is clear, that this is a circular argument, as soon as I argue that there cannot be a juridical definition of both phenomena, since they cannot be distinguished considering the absence of a juridical definition. Furthermore, juridical definitions do not correspond to the empirical world with necessity. In consequence, the existence of a juridical definition does not imply a well-defined or at least well-definable difference between the two either.

However, we can sketch some attributes a juridical definition has to have: as I pointed out, the problem of attribution remains unsolved. Thus, any practical definition has to take this into consideration. Nevertheless, a definition could include ideas of intentions, of intensities and of the complexity of means. While such a definition could work in extreme cases, it offers a large “gray area” again. Hence, a well-definition seems impossible by principle.

The lack of such a definition has, of course, consequences for discourses on cyber war and cyber crime. Both do mix, too. This crossing of borders can be found with many discussions in this field. The most obvious effect is that representatives of the military and of law-enforcement agencies agree on certain demands, especially in the area of surveillance and campaigns against civil rights, foremost against data privacy laws. Another effect is their lamenting that the German separation rule concerning law-enforcement and intelligence agencies or the separation rule for interior and foreign affairs—both emerged out of the German post-ww2 constitution—should be abolished. A serious consequence of the vague difference between cyber war and cyber crime is therefore a militarization of neighboring civilian discourses.