Chapter 13
Cyber Peace: And How It Can Be Achieved

Reto Inversini

Abstract This contribution investigates elements of cyber conflicts and attacks to determine the current state of cyber peace. The first section examines the current state of the Internet and whether or not it is in a state of cyber war. It analyses the classical concept of peace and war and determines which elements can be adapted to the digital sphere and where such a transformation can be problematic. The term 'cyber peace' is then defined and the components that make such a state possible identified. The last section discusses the different roles and their responsibilities to reach and preserve a state of peace in the digital sphere, coming to the conclusion that the Internet is not in a state of cyber war but more in a state of negative or unstable peace. To protect the Internet as a critical infrastructure from being abused as a new battleground, this chapter suggests moving towards a state of stable peace, and proposes increasing the security and resilience on a technical level and building up trust between all actors, ranging from the individual to the state level.

Keywords Attribution · Collaboration and information sharing · Confidence-building measures · Cyber conflict · Cyber espionage · Cyber war · Digital sabotage · State-sponsored actors · Trust and confidence

13.1 Cyber Conflicts of Today

Cyber war is an often-used term in current media and scientific publications. There is much controversy regarding whether it is something real or likely to happen in a near future or if it is a chimera originating from a misunderstanding of the digital sphere.

R. Inversini (✉)
Computer Emergency Response Team (GovCERT) of the Swiss Government, Bern University of Applied Science, Bern, Switzerland
e-mail: reto.inversini@lab42.ch

M. Christen et al. (eds.), *The Ethics of Cybersecurity*, The International Library of Ethics, Law and Technology 21,
https://doi.org/10.1007/978-3-030-29053-5_13

Richard A. Clarke argues that the preparation for cyber war has already begun and that powers such as the U.S., China or Russia are making efforts to plan for such actions:

> It is cyberspace and war in it about which I speak. On October 1, 2009, a general took charge of the new U.S. Cyber Command, a military organization with the mission to use information technology and the Internet as a weapon. Similar commands exist in Russia, China, and a score of other nations. (Clarke 2010, p. x–xi)

Thomas Ridd, in contrast, argues that cyber war did not take place and is unlikely to happen soon:

> It is meant rather as a comment about the past, the present, and the likely future: cyber war has never happened in the past, it does not occur in the present, and it is highly unlikely that it will disturb our future. (Rid 2013: xiv)

Both authors use well-known events such as the Distributed Denial of Service (DDoS) attacks in Estonia in 2007 (Schmidt 2013), but come to different conclusions. Both lines of arguments have their strengths but also their shortcomings. However, we neither have a clear definition of what cyber war is nor do we know enough about the implications such a war would have. Therefore, we prefer to use the term 'cyber conflict'.

Whether events from the past such as the DDoS attacks in Estonia, digital sabotage such as Stuxnet (de Falco 2012) or ransomware outbreaks such as NotPetya[1] are already warlike situations is not the crucial question. In contrast, it is of pivotal concern how we avoid such incidents or even more devastating attacks in the future. In the following, we introduce a concept to make the Internet a more secure and peaceful place.

We can divide the moral aspects of war roughly into one of these three categories: Pacifism, Real-ism and Just War (Walzer 1978; Orend 2006). Pacifism denies any morality to war, and a pacifist must refrain from any involvement in a war. Realism believes that war by itself is something amoral and we can neither judge war, nor can it be guided by moral principles. The Just War theory claims that under certain circumstances, a war may be justified and there are rules to follow to start and lead a war in a morally acceptable way. It goes back to Greek and Roman philosophers and lawyers and since then has evolved and was influenced by Christian theology. There have been many wars that did not fulfil the Just War principles and the Just War Theory has been debated and needs adaptions (Brough et al. 2007). Nevertheless, it forms the base of current international norms such as the UN Charter, The Hague Conventions and the Geneva Convention. Therefore, we use the concept of Just War as the basis for this chapter.

[1] Crowdstrike, NotPetya Technical Analysis; https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ (last access July 7 2019).

War would need to follow several principles[2] to be justified and not violate international law:

- There must be a cause for war that must be declared by a legitimate authority.
- War must be waged with the right intentions and a just cause.
- The probability of success must be determined; there must be a justifiable ratio between gain and loss and it must be the last resort.

These principles form the *Jus ad Bellum*, the right to go to war. The guiding principles of Jus ad Bellum are difficult to adapt to cyber space:

- In order to declare war, one must know one's enemies. This is relatively easy in the physical world even though the number of cases where states hide behind mercenary organisations is rising because it allows them to deny any direct involvement. There are more difficulties inherent in identifying the attackers in the digital sphere: Most states deny any involvement in actions that might be considered as acts of war in the cyber space. It is easy to hide behind proxies, to place false flags and to act on behalf of someone else. Attributing attacks correctly is therefore one of the most important things to address in the digital sphere.
- The Jus ad Bellum allows a country only to go to war if the chances of success are high enough, especially regarding the estimated number of casualties. The probability of success and the number of fatalities are difficult to predict as there are many unknown factors that influence the outcome and because casualties can also be indirect.
- Only national self-defence and humanitarian need are considered acceptable causes for war. To exercise the right of self-defence, a nation-state needs to prove that the event is an armed attack that threatens the state's sovereignty and independence and that another state conducted the attack. In the context of incidents in the digital domain, situations exist where the impact may be obvious such as disruptive or destructive attacks against critical infrastructures, but the problem of who is to blame for an attack remains.
- An important part of the Jus ad Bellum is the concept of territorial and political sovereignty of a state. If a state's sovereignty is in danger, the state has the right to defend itself. Political sovereignty can be easily endangered, but it is difficult to define the threshold where such attacks would justify the right of self-defence. The attackers may try to destabilise a state, e.g. by spreading wrong information or by attacking the political system. This can be done by influencing elections, either by manipulation of the infrastructure or by digitally intruding a disfavoured party. The influencing of public opinion and even elections is nothing new and has been done before the digital era. However, with the use of social media, it has become much easier to directly or indirectly influence large parts of a country. The concept of territorial sovereignty is important but difficult to adapt

[2] Beyond Intractability Knowledge Base, Jus ad Bellum, https://www.beyondintractability.org/essay/jus_ad_bellum (last access July 7 2019).

> to the digital sphere, as there are no physical borders, notably when dealing with distributed systems or applications that use any kind of cloud technology. Scholars and practitioners have written The Tallin Manual on behalf of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE; Schmitt 2017). It describes how international law can be applied to cyber conflicts. Rule 81 states that "Cyber operations are subject to geographical limitations imposed by the relevant provisions of internal law applicable during an armed conflict (Schmitt 2017: 378)." In the second part of the rule, the authors state that these restrictions may be difficult to implement: "Restrictions based on geographical limitations may be particularly difficult to implement in the context of cyber warfare. For instance, consider a cyber-attack using cloud computing techniques. Data used to prosecute the attack from one State may be replicated across servers in a number of other States, including neutral States, but only observably reflected on the systems where the attack is initiated and completed (Schmitt 2017: 378)."

If we consider the goals of a traditional war, there are some interesting differences between a traditional war and a cyber-conflict:

- A traditional war has the goal of conquering territory, accessing resources or gaining political control over the adversary.
- In the digital sphere, no defined territory exists, and digital battles are not about gaining resources. However, a digital war may be used as a supportive element of a traditional war to seize territory or resources. This may be a sign that in most cases, hostile digital actions are part of a larger scenario that also includes more traditional elements of war.
- It is possible that we will only observe actions in the digital domain when a state wants to gain political control over another state. This leads us back to the concept of political sovereignty, which will become increasingly important.

We believe it is likely that most hostile actions in the digital sphere will not take place in the context of officially declared wars. This is not a result of the ongoing digitalisation but reflects a more general trend: As Fazal states, there has been a sharp decrease of war declarations since the 1950s:

> From 1950 on, by contrast, the number of wars remained about the same, but the number of wars accompanied by declarations declined dramatically—to three. Declaring war—an institution that has typically accompanied the outbreak of hostilities since at least the Roman Empire—appears to have fallen out of states' repertoire of behaviors. (Fazal 2012: 557–558)

If we consider this and accept the difficulty of attribution beyond any reasonable doubt, we do not expect that countries will declare war formally, especially for cyber operations. Without a war declared and without an independent and accepted attribution, the prerequisites of Jus ad Bellum are not fulfilled. In the future, more situations that resemble a war or are characterised by high tensions will emerge, but they will not meet the criteria mentioned above.

This is why we include not only the case of declared war into our considerations but any action that violates the sovereignty of a state. Rule No 4 of the Tallin Manual

states that no violation of the sovereignty of another state is acceptable (Schmitt 2017: 16–18): "A state must not conduct cyber operations that violate the sovereignty of another state."

The comments to Rule No 4 describe various cases where the experts agree that a violation had occurred such as if the cyber operation damages an infrastructure on the territory of another country (Schmitt 2017: 18) or if governmental functions of a state are impaired by a cyber-operation of another state (Schmitt 2017: 22). One basic precondition of a violation of sovereignty is that it must be attributable to another state. This gets progressively complicated as governments hire mercenary groups to carry out attacks in the digital sphere. This allows a country to deny any direct involvement in a conflict.

Using so-called cyber proxies (Maurer 2018) or cyber mercenaries can be attractive to governments as they provide expertise and plausible deniability that a state has any direct involvement. In the past, we have seen two types of such actors: hacktivist and commercial organisations. Mostly, actions performed by such groups may be illegal from a penal point of view but cannot be considered as acts of war. However, there are actions that increase the tension between conflicting parties and that lead to an escalation into a warlike situation. It is likely that the use of such groups will rise as their use is too tempting for governments. They can be a cheap yet effective alternative to regular soldiers acting in the cyber space and provide more deniability in case an attack is discovered and analysed. George Lucas (2017: 28) believes that the danger of such groups is underestimated and may pose a serious threat in the future.

We believe the use of such organisations will increase the likelihood that warlike situations will be of longer duration without a formal war being declared, as such groups tend to engage in war for their own benefit (political influence or commercial interests). During wars that relied largely on mercenary armies such as the 30 Years War, at least a part of the financing of the soldiers was done by robbing civilians. Even though not directly comparable, the overlapping of digital crime and state-sponsored hacktivism resembles this situation and might get progressively important, as states could offer impunity to cyber criminals in return for digital attacks which are in the interest of the state. The authors of the Tallin Manual explain that non-state actors cannot violate the sovereignty of a state but that the targeted state may nevertheless react to harmful attacks following international law (Schmitt 2017: 18). We believe the differentiation between state and non-state actors is becoming increasingly difficult. This uncertainty might eventually lead to situations with a high risk of escalation if a state responds with force to attacks of non-state groups and, by doing so, violates the sovereignty of another state.

Although we believe it is wrong to infiltrate other networks to gain information illegally, such attacks are not necessarily acts of war. Espionage has always existed, even during peace times and sometimes it has even helped to preserve peace: It gave the other party information about what the enemy has planned and thus improved the predictability, which helps to define the course of action. However, the uncontrolled use of espionage may destroy trust. As cyber espionage seems to become

epidemic, state actors should be cautious and should refrain themselves from too-frequent spying.

13.2 Cyber Peace

The contrastive term of cyber war is 'cyber peace'. Often, peace is defined in a negative way as the absence of war. Boulding defines peace in both ways:

> The concept of peace has both positive and negative aspects. On the positive side, peace signifies a condition of good management, orderly resolution of conflict, harmony associated with mature relationships, gentleness and love. On the negative side, it is conceived as the absence of something, the absence of turmoil, tension, conflict and war. (Boulding 1989: 3)

We define cyber peace in a manner that considers both aspects. We should not define peace just by the absence of conflict and war, as these elements may be visible in the physical world but not in the digital sphere.

Peace can have various states that are defined in different ways, e.g. by Alexander George (1998: p. ix) as precarious, conditional and stable, by Miller (2017) as cold, normal and warm, or by Kacowicz et al. (2000) as negative peace, stable peace and pluralistic security communities. These definitions have much in common. We use the definition by Kacowicz et al. (2000: 21):

> A zone of negative peace (mere absence of war) is one in which peace is maintained only on an unstable basis and / or by negative means such as threats, deterrence or lack of capabilities to engage in violent conflict at a certain time. (…) A zone of stable peace (no expectations of violence) is one in which peace is maintained in on a reciprocal and consensual basis. (…) A pluralistic security community of nation-states, with stable expectations of peaceful change, is one in which member states share common norms, values and political institutions; sustain a common identity; and are deeply interdependent.

13.2.1 Current State of Cyber Peace

The Internet is still in the zone of a negative peace: Current operations are not very violent, but there is an imminent risk of an escalation.

We may understand the current state of the Internet in a similar way as the frontier area in the Wild West. The absence of regulation, the quick emergence of new ways to earn money, and the fact that most effective security for the participants does not come from the state but from private organisations are all elements that show similarities with a booming frontier town. We have witnessed the rapid development of new technologies and the emergence of a new and global form of criminality and state sponsored espionage and even destructive attacks. However, in most cases, the damage was still limited and often it was not inflicted on purpose but was

a collateral effect caused by underestimating the interconnectivity of the Internet and the low security precautions.

A good example of the uncertainty about the current state of the Internet, and whether we are already near a state of cyber war is the aforementioned NotPetya case. There has been considerable discussion over whether this attack could already be considered as an act of war. While NotPetya caused substantial damage, we believe it is not an act of war as it lacks most of the prerequisites we have mentioned above. NotPetya is a malware that is based on the leaked National Security Agency (NSA) exploit 'Eternal Blue'. One hypothesis is that NotPetya was aimed at infrastructure elements in the Ukraine. It spread like wildfire and hit many big organisations such as Merck or Maersk. This was possible because systems were neither patched against known vulnerabilities nor isolated from other networks. However, governments and media treated the case like a hostile action that was at least at the border of an act of cyber war.[3] This case displays a few interesting elements:

- If a state stores and uses 0-day vulnerabilities,[4] there is a risk that someone else uses it against e.g. critical infrastructures.
- In most cases, attackers exploit bad security practices.
- For affected organisations, it is often favourable to make the attack bigger than it was to distract attention from its own failure to secure its systems properly.

NotPetya was an attack with a big disruptive effect that endangered many organisations and—under bad preconditions—could have been the starting point of an escalation. However, this attack was only possible because organisations neglected basic security and not because the attack was remarkably skilful. We can therefore learn from this case that with proper security precautions, attacks become much harder to conduct and the risk of collateral damage drops. As many critical infrastructure elements are being connected to the Internet without appropriate security controls, offensive actions are often perilous, as no-one can limit actions to the intended target. To maintain a stable cyber peace, information and communication technology (ICT) operators must assume their responsibility for building and maintaining secure and resilient systems.

Attacks with a global impact are possible and there is a high risk associated with this. As no specific de-escalation procedures for the digital sphere are in place on the state-level, the risk of an escalation which eventually could lead to hostilities exists and we should not underestimate it. If too many unfavourable political elements come together, such an attack might be the starting point for a rapidly escalating situation that nobody ever intended but that could cause a lot of harm.

---

[3] The Independent, Britain has entered 'new era of warfare' with Russian cyber-attacks, Defense Secretary warns; https://www.independent.co.uk/news/uk/home-news/russia-cyber-attacks-notpetya-gavin-williamson-defense-secretary-putin-hacking-ransomware-a8212801.html (last access July 7 2019).

[4] A 0-day vulnerability is a vulnerability that has not yet been publicly disclosed and for which no security patches yet exist but that is known to persons and organisations that are willing to exploit it. Day 0 refers to the day the programmer/manufacturer of the software affected learns about the vulnerability.

The Internet is currently in a state of a negative peace. We have a good chance to move towards a stable peace if we can increase collaboration and trust between the different actors. We should act on different levels to stabilise the cyber space and to reduce the likelihood and impact of hostile actions.

13.2.2 How to Achieve a State of Stable Cyber Peace

It is not reasonable to believe war and conflicts can be completely avoided in the near future. However, it is possible to reduce the likelihood and the impact of conflicts, both in the real world and in the digital world, thus moving from the state of a negative peace to a stable peace. Luckily, there are already several elements in place that will help us achieve this goal (see also Chap. 18):

- All participants are highly interdependent, which leads to some degree of restraint in attacking others, as there might be a backlash on their own network.
- Common norms (the Internet protocols) and values (the Netiquette[5]) are in place and widely accepted.
- There are defensive organisations working together and trying to increase the security and stability of the Internet: Computer Emergency Response Teams (CERT) exist on various levels ranging from organisational CERTs to National CERTs. Sometimes they even form permanent, supra-national groups such as the European Government CERTs group (EGC[6]) where various national CERTs of Western Europe co-operate and share information about digital threats.

To achieve a stable peace, we must invest in defensive measures on all levels. While offensive capabilities may serve as a deterrence because the attacker fears retaliation, defensive measures reduce the likelihood and the impact of a successful attack. In the following, we highlight the two most important components of a stable cyber peace: security (including resilience) and trust.

On a technical level, security and resilience are the most important factors that help us reduce the likelihood and impact of digital attacks. The higher the security and resilience are, the more trustworthy the infrastructure is. Trust is important as the glue between the actors in the digital sphere and is important for collaboration and confidence. Based on security and trust, states have enough reason to exclude the risk of being attacked from their top priorities because enough protocols, processes and treaties are in place that form a stable peace.

[5] Netiquette RFC

[6] European Government CERT Group

13.3 Security and Resilience

Security defines the technical and organisational measures that are implemented to reduce the risks to the digital infrastructures of a country. Resilience is a close relative but also includes passive elements and is more geared towards withstanding and quickly recovering from attacks. While an attacker only needs to make one single, successful attack with reasonable costs and low risk, defending all the critical infrastructure of a country is extraordinarily hard to achieve. In contrast to the nuclear arms race, cyber-attacks are not that devastating, even though one should not ignore the potential impact of a cyber-attack due to collateral damage and unwanted escalation. This may lead to a much quicker and light-headed execution of such attacks and a lower rate of mutual deterrence. It is possible to recover from such an incident if proper design and planning of defence is in place. As Joseph Nye puts it: "Redundancy, resilience and quick reconstitution become crucial components of defence" (Nye JS Jr 2018: 5).

Large parts of the Internet are vulnerable to attacks, starting with routers and data centre switches that have received no security patches for years, to outdated operating systems and middleware up to content management systems and web applications that have many well-known vulnerabilities (see also Chap. 2). This gives adversaries the advantage of having many opportunities to attack systems, abusing them as jump points for their operations and thus covering their tracks. An attacker may choose between various attack vectors, infiltrate the systems and networks and achieve his goals. One single weak spot may be sufficient for the perpetrator to enter the network while the defenders need to guard many systems, often without adequate resources. We can therefore conclude that there is a disequilibrium between offense and defence; or as George Lucas (2017: 127) states: "The advantage, as the cybersecurity experts themselves admit, always lies with the offense" (see also Chap. 12).

An illustrative example is the emergence of so-called Internet of Things (IoT) devices which are mass-produced cheaply; their users often connect them to the Internet with no security measures taken (e.g. keeping default passwords active). Criminals abused the resulting attack surface to build an enormous botnet (Mirai Botnet; Antonakakis M. et al. 2017), which successfully attacked one of the largest Domain Name System (DNS) providers (DynDNS). As many companies use the DNS services DynDNS provides, the attack led to outages in the U.S. and also in Europe. This case showed two things:

– There is a huge number of vulnerable devices on the Internet that can be abused for attacks.
– The centralisation of services often leads to a large impact of a successful attack and destroys parts of the design target of having a resilient Internet.

The disequilibrium between offense and defence is true at the moment, as the attacker has to find one weakness for a successful attack while the defenders must protect a plethora of systems, some of them being legacy systems that no longer

receive security patches. However, we are convinced that Joseph Nye's statement is not true in its absoluteness, as there are also advantages on the defender's side:

- We should not underestimate the complexity of the attacker's task: The defenders have a good oversight of their networks and are disposing over advanced monitoring systems. The attacker, in contrast, must peek through a keyhole (one or more infected systems) and try to sort out the interesting data and systems without making too many errors and getting discovered.
- Every attacker makes mistakes and the forensic exchange principle of Locard (Tilstone et al. 2006: 59) ("Every contact leaves a trace") is also true in the digital sphere. It is up to the defender to find these traces as fast as possible to detect the attacker before severe damage occurs.
- In case of attacks against Industrial Control Systems (ICS), the attacker must have special knowledge not only about the overall functioning but over the actual implementation as well. It is a time and money-consuming task to achieve such knowledge and attackers can only do this if the price is worth it.

The advantage of the attacker should not lead to an arms race that neglects the defence ("why invest in defence, if the offense always has the advantage?"). In contrast, we must strengthen the overall security of Internet connected devices and the resilience of critical infrastructure. In many incidents, such precautions would have prevented or at least delayed the attack. The better the security, the higher the price for successful attacks becomes and thus this makes attacks less likely. It also helps to reduce the probability and impact of collateral damage that has not been intended by the attacker but could lead to a dangerous escalation by itself.

With digital sabotage, one of the biggest advantages in the digital sphere lies in the fact that restoration of the destroyed IT infrastructure can often be done fast and without high costs. However, this requires a well-thought design of infrastructure and data as well as the usage of technologies for the rapid restoration of data. This is extremely important for critical infrastructure such as electricity, water and health services. The emphasis lies on the term *quick restoration,* as a restore procedure that would take days is often too long, notably in organisations where timely access to current data is crucial, such as hospitals. It is also essential to separate the different data stores so that an attacker who destroys (encrypts, deletes or modifies) data cannot access the second storage with the data that is going to be restored. While these requirements are challenging, there are technical options to building and operating such a system. One interesting case has been documented in a hospital in the USA where the management decided to pay the ransom even though backups would have been available.[7] However, restoring all data and systems would have taken too long, as the outbreak of the ransomware had been very widespread throughout the hospital's network. It gets more difficult if the digital attack leads to physical damage, e.g. of devices that are overloaded by the attackers. To reduce such impacts, the user

[7] Bleeping Computer, Hospital Pays $55 K Ransomware Demand Despite Having Backups, https://www.bleepingcomputer.com/news/security/hospital-pays-55k-ransomware-demand-despite-having-backups/ (last access July 7 2019).

must not blindly interconnect the digital sphere with the physical world but should have well-defined gateways. The user should always define reasonable boundaries that trigger an alert or force a system to go into a 'fail-safe' state and wait for a human intervention.

We would therefore like to emphasise the importance of building up strong and resilient infrastructures that are designed and operated by organisations with mature security processes. We believe there must be an incentive by the state to lead the development of digital technologies in the right direction as there is still too little stimulus for enterprises to write secure software. This can either be on the regulating side, by enforcing minimal security standards for every device connected to the Internet, or by having better product liability for software.

13.4 Trust and Confidence

Trust is a crucial element for inter-personal relationships or between smaller groups of people that share common values and follow common goals. Interpersonal relationships form the base of any stable peace in a society and between nations. The better the citizens know and trust each other, the greater the confidence between their nations is. It forms the base for security, collaboration and information sharing for their mutual benefit.

There already exist many trust relationships between persons working in the domain of cybersecurity who collaborate across national and cultural borders and are building invisible trust networks globally. To build up such a trust relationship, collaboration and sharing of information must be fostered on all levels between all participants. This raises the bar for successful attacks, thus making them more unlikely. Trust is the key precondition for collaboration and sharing of information. Without trusting someone, no-one shares valuable information, and without sharing information, it is difficult to increase the trust level between individuals and organisations. We therefore propose to work together and share information in areas where a common understanding already exists. A good example is the domain of combatting cyber-crime, where we can begin to build up the trust and then also increase the collaboration in areas that are much more sensitive, such as state-sponsored activities.

The collaboration and sharing of information must take place on various levels:

– Between states: There are some promising efforts such as EGC (Group of European Government CERTs) or IWWN (International Watch and Warning Network). However, much of the collaboration happens only between partners that share the same values and often already have some kind of political alliance. This is understandable and only underlines the importance of trust. There is a broad understanding that in law enforcement an urgent need to exchange information in a much quicker way exists. There are international agreements such as

the Convention of Cyber Crime of the European Council that help to improve the situation (see also Chap. 18).
- Numerous interest groups and volunteer organisations are already fostering the exchange of information between individuals, non-profit organisations and commercial organisations. We must support these efforts, as many of these persons and organisations have a deep understanding of how the digital sphere works and are the best bet for effective and efficient measures to secure the Internet.
- Critical infrastructures are crucial for the safety and stability of a society. Without a reliable provisioning of electric power, water, food and health care, societies are rapidly destabilised. We must improve information exchange between the critical infrastructures not only within a nation's border but also throughout the sectors on an international level.

Trust forms the confidence between the various actors, who can be confident that no unexpected acts of violence might occur and that there is a common perception on how actors react in certain situations. Without confidence, states and organisations are constantly on guard, watching out for hostile actions. In an area as complicated as cyber space, chances for misinterpretations and escalations are particularly high. The lack of confidence that no other nation will use digital weapons against one's own nation is also something that describes the current situation rather well. We must have a mutual basic level of confidence that no unexpected behaviour takes place. This can be achieved by defining and implementing confidence-building measures (CBMs):

> The ultimate goal of CBMs is to strengthen international peace and security by reducing and eliminating causes of mistrust, fear, misunderstanding, and miscalculations. (Healy et al. 2014)

The effects of a full-scale cyber conflict are not that clear even if the potential for damage might be huge. We should therefore not neglect the risk of an unplanned and unwanted escalation. Even though not directly comparable, we can gain important insight from the era of the Cold War, with its danger of an imminent nuclear war. Joseph Nye (2011) summaries the similarities between that era and our time of cyber conflicts as follows (Nye JS Jr 2011):

- superiority of offense over defence
- use of weapons for tactical and strategical purposes
- possibilities of first and second use scenarios
- possibility of automated responses

It is challenging to define what a digital weapon is: Although it is rather clear for the case of nuclear weapons, this is much more difficult in the digital sphere: Many things that can be considered as cyber weapons have their origins in dual-use goods (this is especially true for vulnerability scanners and similar tools).

One of the most important and successful measures implemented for reducing the likelihood of a nuclear war were CMBs. We believe that CBMs could reduce the

probability of an escalation in a cyber-conflict as well. In the following, we try to deduce similarities and differences for CMBs in the digital domain:

- To avoid misunderstandings, it is important to exchange information about troops, assets and their movements. This helps to avoid incorrect assumptions about the capacities of the other party and may help to reduce the speed of an arms race. This is much more difficult to achieve in the digital world, as most nations keep their capabilities secret and as there is an overlap between intelligence services, 'traditional' troops and unofficial combatants.
- Exchange of personnel/conducting joint exercises: This helps to build up a personal relationship between the participants that supports to build up trust. To some extent, this is already being done as many cybersecurity professionals meet at regular intervals and on conferences. However, for military troops, this mostly exists between friendly countries or allies such as NATO and not between potential adversaries.
- Improving predictability helps gauge unclear and fierce situations in a better way. This reduces the likelihood of unwanted escalations and helps to contain difficult situations quickly and efficiently.
- Enhancing transparency of involved parties leads to a better understanding of a conflict and reduces the risk of inadvertent escalation. Even though satellite surveillance and other reconnaissance helped to improve transparency in large classical conflicts, there are still situations where the involvement is not clear and where parties indirectly take part in a conflict, such as during the Ukraine crisis. In the digital sphere, this is even more demanding as there it is nearly impossible to verify which parties are involved in a digital operation.
- Military actions against critical infrastructure or against civilians should be restricted. During conflicts between two states, there are many regulations in place to reduce casualties of civilians and to spare infrastructures such as hospitals. In the digital sphere, this is much more complex, as it is often unclear whether a resource belongs to a legitimate target, to a civilian or even to a hospital. We must accept that there is always a large risk of unwanted collateral damage due to the strong interdependencies on the Internet. This should lead all participants to refrain from offensive actions as much as possible.

Confidence partly relies on the capability to trace down the identity of an attacker beyond a reasonable doubt. This leads us again to the problem of attribution in cyberspace. Evidence is hard to gain and tracks often end at legislative borders. Additionally, attackers can introduce wrong traces that point to another Nation/organisation ('false flags') which may lead to false accusations and in what follows to increased tensions and even real conflicts. Therefore, it is important that parties not involved in the conflict and with enough reputation, technical skill and independence are responsible for the attribution so that the public and the involved parties both accept the verdict. This is extremely challenging. Apart from some approaches

in an early stage (e.g. a proposal by Microsoft for such an attribution organisation[8]), we are far away from such a situation. A correct attribution is pivotal to respond with force against the adversary, but traces are seldom obvious and unambiguous. Any attacker may insert enough information to blame someone else for the attack. This also bears the risk that state sponsored groups are more willing to attack for various reasons. If they can seed false traces, politicians might use such false flag operations to justify offensive actions during a political crisis.

Even though we have shown how difficult it is to build up higher confidence between potential adversaries in the digital sphere, first steps have been made in this direction:

- A good example is the establishment of the first multilateral cybersecurity related agreement by the Organisation for Security and Co-Operation in Europe (OSCE) in 2013.[9]
- A second set of CBMs was decided upon in 2016.[10]

It is beneficial for the security of the Internet and all its participants if policy makers continue on this path and increase their efforts to reach a stable cyber peace.

13.5 Roles and Responsibilities

We cannot achieve cyber peace without everyone taking their own share of responsibility. We do not describe every actor and his or her role in detail but rather mention a few cornerstones:

13.5.1 Policy Makers

We need to differentiate between policy making on an international level and on a national level. On an international level, multinational organisations such as the United Nations Organisation (UNO) or Organisation for Economic Co-operation and Development (OECD) are important actors that can forge a path to a cyber peace in the longer term. For short-term and operational issues, we propose strengthening existing organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN), the Regional Internet Registries (RIRs), the Internet Engineering Task Force (IETF), Forum of Incident Response and Security Teams

[8] Microsoft, an attribution organisation to strengthen trust online, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QI (last access July 72,019).

[9] Organization for Security and Co-operation in Europe OSCE, Permanent Council Decision No. 1106; www.osce.org/pc/109168 (last access July 7 2019).

[10] Organization for Security and Co-operation in Europe OSCE, Permanent Council Decision No. 1202; www.osce.org/pc/227281 (last access July 7 2019).

(FIRST) and Trusted Introducer (TI). These already have a strong understanding of how the Internet works and are not subject to quickly changing political situations.

Similar to the case of nuclear weapons, one strategy could be that an increasing number of states decide to refrain from possessing digital weapons with destructive capabilities or at least to guarantee they are abstaining from the first use of such weapons. Although this might be an interesting approach, it is also very difficult, as such a treaty can hardly be controlled and as there is a big overlap between the tools state-sponsored organisations and criminal groups are using. At the very least, states should define and adhere to rules of engagement in the digital world that ensure no state attacks the critical infrastructures of another state in order to avoid causing civilian casualties.

States are strongly challenged when it comes to digital crime and state sponsored actions. As these actors operate from different locations and have their infrastructure in various countries that they may change swiftly, a purely national approach is doomed to fail in most cases. The most efficient way to address these problems is via international cooperation. A step forward has been taken by the Convention on Cybercrime. Its aim, set out in the preamble, is to pursue a common criminal policy aimed at protecting society against cybercrime by adopting appropriate legislation and fostering international co-operation.[11] Initially driven by the Council of Europe, 57 other countries have signed and ratified the treaty as of 2018.

On the national level, many nations have been developing National Cybersecurity Strategies. Policy makers should try to strengthen the defence before investing in offensive capabilities. Even though many countries try to overcome their weaknesses by having offensive capabilities, we believe this is not a well-thought-out approach. It assumes that in the case of an attack it is clear who is attacking (which seldom is the case) and that striking back can solve the problem and does not lead to an escalation with much collateral damage. One of the best investments any nation can do is making the Internet, and the systems connected to it, more secure and resilient. We therefore encourage policy makers to focus on the hard groundwork of securing the Internet and not so much on building cyber commands and capabilities that cannot address the underlying problems.

The state should be in charge of providing reasonable security for everyone and free of charge by ensuring basic Internet security and resilience as well as combatting criminal groups. All citizens must be able to use the Internet free of fear and with a low risk of being the victim of an attack. This is one of the most important tasks a state must fulfil. If it fails in doing so, only persons and organisations with enough financial and/or intellectual resources can protect themselves. This would violate any principle of fairness and the state would risk losing its monopoly on the use of force, which is a basic principle of any constitutional state.

[11] Council of Europe, Treaty No. 185, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (last access July 7 2019).

13.5.2 The Society

As a society, we must adapt our own perception of risks and values to the new digital era. We should be careful when we are transferring concepts of the traditional world into the cyber domain and should always question their suitability. The generations to come will have a better understanding of the risks involved, as they are growing up using these technologies. We should foster this by not only teaching the technology but also the values associated with it. Societies should try to understand the Internet as a common good of humankind and not as something restricted to state or cultural boundaries.

13.5.3 The Private Sector

It is difficult to draft one role for all companies, as these are very diverse. In any case, they must secure their systems according to best practices and should avoid trying to reduce costs by using insecure systems, applications and procedures.

If a company has a critical role in a society, such as being part of the health care or energy sectors, there are additional points it must adhere to: Its IT department must protect the systems and data against any kind of sabotage and disruption and fulfil requirements set up by the regulator; it needs to detect intrusions quickly and needs to provide effective security incident response and recovery procedures; and it should closely monitor the threat landscape and be capable of quickly adapting to new threats.

Companies that sell security products and services have special roles and responsibilities as well. Without commercial security companies, the Internet would be much more dangerous and unstable as they provide security products that help organisations and individuals protecting their networks and systems. However, there are companies that act as mercenary groups or that export digital weapons into areas of conflict. These groups may put a stable peace in danger. We propose having guidelines about ethical behaviour that are co-developed and complied with by security companies. We believe that self-regulation is a promising approach, but that in case of a violation of these guidelines, sanctions are also necessary.

13.5.4 The Individual

Due to the high degree of interconnection, every participant on the Internet has a special responsibility towards the other users. If someone does not properly secure his system or application, he or she might be abused as a first attack vector for actions that eventually lead to substantial damage. The following scenario shows a possible sequence of events:

– A poorly secured website of a local restaurant is hacked by a state-sponsored attacker group.
– Employees of a nearby-located critical infrastructure (CI) repeatedly visit this restaurant and its webpage to read the current menu.
– The attackers abuse the website as a waterhole for infecting the employees of said infrastructure.
– The intruders have now gained their first foothold in the network of the CI and they can use the server for the exfiltration of the stolen data. It is difficult for intrusion detection systems to recognise such traffic, as it is expected and already known.

As it is not a workable solution that everyone taking part on the Internet can take full responsibility for securing his or her systems, all actors on higher levels must try to absorb these risks by implementing additional safeguards.

13.6 Conclusion

In this chapter, we discussed the current state of the Internet as a negative yet unstable peace and demonstrated the most important components for reaching a stable peace. These components require increasing confidence and trust between all participants, which is mainly a political and psychological topic. The elements formed around security and resilience are more focused on technology but also include strategic, political and economic elements.

We can achieve a stable cyber peace if most participants consider the Internet as being a space shared with others that has comprehensible and documented rules to protect its users from damage —be it physical or digital. This leads to the need for an international system of norms, rules of engagement, best-practices and responsible behaviour of individuals, enterprises and states.

It is important to note that there are already many safeguards and processes in place. These limit the actions and the impacts of state-sponsored actors and of criminals, and help secure the Internet in approaching a state of a stable cyber peace. This multi-level approach attempts to solve the problems where the chances are highest for doing so. Shackelford describes this as a "polycentric" approach:

> Private-sector cybersecurity best practices, along with national, bilateral, and regional bodies acting as norm entrepreneurs that are identified throughout this study are together conceptualized as components of a 'polycentric' approach to promoting a global culture of cybersecurity. (Shackelford 2017: 7)

We believe it is crucial to keep and foster this approach and to extend it as much as possible to ensure peace on the Internet and to prevent actors from using it as a new battleground. It is important to not try to transfer concepts and procedures from the physical world to the digital sphere without questioning their suitability. Even though it is very unlikely that the Internet will be a sphere without conflicts, we can

nonetheless make it much more secure and resilient. This reduces the likelihood of devastating attacks, which in turn could lead to a dangerous escalation. Every step we make towards a more stable peace in the digital sphere helps protect the Internet, critical infrastructures and our society as a whole.

Acknowledgments The chapter was created with funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700540 and the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 16.0052-1.

References

Antonakakis M et al. (2017) Understanding the Mirai Botnet. https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf. Last access 7 July 2019

Boulding KE (1989) Stable peace. University of Texas Press, Austin

Brough M, Lango JW, van der Linden H (eds) (2007) Rethinking the just war tradition. SUNY series, Ethics and the Military Profession

Clarke RA (2010) Cyber war: the next threat to national security and what to do about it. Ecco

De Falco M (2012) Stuxnet fact report. Available at: https://de.scribd.com/document/181049284/De-Falco-Marco-CCDCOE-Stuxnet-Facts-Report-A-Technical-and-Strategic-Analysis-pdf. Last access 7 July 2019

Fazal TF (2012) Why states no longer declare war. Secur Stud 21(4):557–593

George A (1998) Foreword in Europe undivided: the new logic of peace in U.S.-Russian Relations

Healy J, Mallery J, Tothova Jordan K (2014) Confidence building measures in cyberspace. http://www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf. Last access 7 July 2019

Kacowicz A, Bar-Siman-Tov Y, Elgström O et al (2000) Stable peace among nations. Rowman & Littlefield Publishers, Lanham

Lucas G (2017) Ethics and cyber warfare: the quest for responsible security in the age of digital warfare. Oxford University Press, New York

Maurer T (2018) Cyber mercenaries: the state, hackers, and power. Cambridge University Press, Cambridge

Miller B (2017) International and regional security: the causes of war and peace. Routledge, London

Nye JS Jr (2011) Nuclear lessons for cyber security. Strat Stud Q 5(4):18–38

Nye JS Jr (2018) Cyber power. https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf. Last access 7 July 2019

Orend B (2006) The morality of war. Broadview Press, Peterborough

Rid T (2013) Cyber war will not take place. C Hurst & Co Publishers Ltd, London

Schmidt A (2013) The Estonian cyberattacks. Atlantic Council, Washington, DC

Schmitt MN (ed) (2017) Tallinn manual 2.0 on the international law applicable to cyber. Cambridge University Press, Cambridge

Shackelford SJ (2017) The law of cyber peace. Chic J Int Law 18(1):Article 1

Tilstone W, Savage KA, Leigh AC (2006) Forensic science: an encyclopedia of history, methods, and techniques. Emerald Group Publishing Limited, Bingley

Walzer M (1978) Just and unjust wars. Basic Books, New York