zebis

Ethics and Armed Forces

Controversies in Military Ethics & Security Policy

Issue 2014/02

Cyberwar: The Digital Front – An Attack on Freedom and Democracy?

Special: Cybersecurity in Germany – Myth and Reality

Read more on www.ethicsandarmedforces.com

Editorial

Countries and governments are increasingly using digital technologies in cyberspace, whether for communication, monitoring, espionage, combating crime and optimization of their military forces.

The freedom of the Internet creates new spaces and facilitates new strategies. But how secure are they really? How secure is our own data, and how safe are countries? Many governments already integrate cyberwarfare methods in their civil and military security strategies.

The German Federal Government has stated the opinion that a cyberattack should only be deemed tantamount to an armed attack under international law if its impact crosses the threshold to an armed conflict and is comparable with that of conventional weapons. However, a specific attribution of "cyber activities" in the broadest sense to this definition poses some difficulties.

The distinction principle of humanitarian international law prohibits use of methods which cause unnecessary suffering. In cyberspace, that could refer to special programs which are specifically used to sabotage critical infrastructure, such as control systems for dams or nuclear power stations. This prohibition would be violated if cyberwarfare were used to damage a nuclear power station in such a way that radiation would cause harm to combatants or the civilian population.

A digital arms race – what efforts are being made internationally to regulate cyberwarfare? Can we call for an "open, secure and peaceful Internet" on one hand, while participating in a militant arms race for the electronic war in cyberspace on the other?

Warfare with cyber weapons raises legal and ethical questions. The authors in this e-journal edition of "Ethics and Armed Forces" write about "Cyberwar: The Digital Front – An Attack on Freedom and Democracy?" from a wide range of different perspectives.

International authors discuss ethics, international law and the militarization of cyberspace, stimulating controversial debates worldwide.

I wish to thank our authors, publishers and editorial team for this issue.

Veronika Bock
Director of zebis

Cybersecurity and Civil Liberties: A Task for the European Union

by Annegret Bendiek

The European Union adopted its cybersecurity-strategy in June 2013. The EU coordinates the national policies of its 28 member states and manages the largest single market in the world. Decisions taken in the EU have a high relevance for the rest of the world. Implementation of the EU cybersecurity strategy brings together very different understandings of the appropriate balance between state and society, security and freedom, and between policy decisions shaped intergovernmentally and by parliaments.

How these views are brought together and which long-term decisions are taken here will decisively influence the new order of cyberspace for years to come. The following questions arise in this regard: How much freedom should the Internet guarantee, what security precautions against crime and terrorism need to exist, and where should the line be drawn between national self-determination and the global sphere? Will there even be a worldwide Internet in the future, or will the emergent trend of web fragmentation continue, bringing greater national control over access and content?

To preserve a balance between a secure Internet and civil liberties, the EU must not stop at simply implementing its cybersecurity strategy, but rather adopt a comprehensive strategy for cyberspace via the community method.

Protection against industrial espionage is an important location factor. Electronic commerce accounts for around four percent of total trade throughout the EU, and is rapidly growing. The Internet also makes a considerable contribution to GDP growth. Estimates suggest that consumers could save a total of more than 200 billion euros through greater use of electronic commerce. But this requires a high degree of trust in online security. Thus around half of all EU countries have adopted national cybersecurity strategies. More than 30 countries now have cyber units within their armed forces. Cyberattacks have become part and parcel of strategic calculations in new computerized conflicts, both between non-state and state actors, and between states.

Security problems are without doubt a major challenge for Internet regulation. However, emphasizing the security aspect and neglecting the idea of cyberspace as a global public good may pose a danger to basic rights and therefore to democracy. Security should not be regarded as a policy topic that is somehow above democracy. How and by what means “critical infrastructures” (energy, transport, health) should be protected, and how private information should be treated while maintaining this protection, are not questions that should be deliberated and decided only by expert committees. These are matters for the *European Parliament* and national parliaments.

Private self-regulation is one instrument. But when it comes to questions of informational self-determination, freedom, and fundamental democratic rights, the only democratically acceptable solution is one which is shaped in accordance with the rule of law and therefore

by parliament. Yet so far calls for parliamentary oversight and legally binding cyber policy arrangements have not been heard either at international or European level.

A comprehensive EU strategy for cyberspace should operate on three regulatory levels:

Global

The existing mode of regulation for the Internet does not sufficiently involve the emerging powers Brazil, India, China and Russia, and is too one-sided in its bias toward the United States. Use of the term multi-stakeholder governance obscures the fact that U.S. interests and U.S. businesses are de facto the main agenda-setters, and financially weaker interests have little chance of asserting themselves in institutions such as the ICANN (Internet Corporation for Assigned Names and Numbers) or IFG (Freedom of Information Law in Germany). Whereas, for a long time, the United States and Europe pulled together to defend the existing model, recent revelations about U.S. surveillance practices have produced increasing European skepticism toward this model. Only a coalition of liberal states will be able to preserve a free and open Internet.

Transatlantic

The EU and U.S. are strongly divergent with regard to their respective cybersecurity policies. While the Americans are increasingly relying on deterrence, the Europeans are pursuing a more police-based approach, aimed at building up resistance. This difference is reflected in the different tasks and competencies assigned to the respective intelligence services, and a corresponding different treatment of fundamental civil rights such as the right to informational self-determination. To stop these differences turning into a massive conflict, both sides need to be much more willing to make concessions to each other. A key condition for successful cyber dialogue is that both sides should acknowledge as fact the domestic political limitations to the transatlantic willingness to compromise. Because of its role as a global enforcer, the United States cannot reduce its emphasis on the security aspects and hence the deterrent dimension of cyber policy, either now or in the future. It is equally true that the EU will continue to focus on combating cybercrime and that data protection issues will remain of paramount importance. Only if both sides respect these limits to cooperation it will be possible to clear the way for mutually beneficial collaboration in global cyber policy.

Transnational

EU cyber policy is faced with a whole host of new transnational conflicts that urgently need to be addressed. Much trust has also been destroyed within society. The revelations have made citizens aware of the flip side of computerization. Many citizens are in danger of losing trust in the security of the Internet, and are responding with growing skepticism and increasing demands for renationalization of communication structures. In connection with TTIP, there are already calls for supranational legal instruments and independent dispute settlement bodies. The European negotiating position includes the demand for public-private dispute resolution mechanisms and hence for a transfer of the community principle into a legal concept which is alien to international policymaking. Not only the European member countries but also the United States and other liberal countries would therefore need to embrace the idea of supranational legal norms in future – whether for data protection or legal recourse against the use of data.

The EU cybersecurity strategy aims to step up cooperation between member states over the years ahead in the area of security tech-

nologies, yet a comprehensive EU strategy for cyberspace should include stronger legal and policy obligations with respect to exporters of information and communication technology. Authoritarian states are increasingly censoring, monitoring and controlling the Internet with the aid of technology provided by European and North American companies such as *Area* in Italy, *Ultimaco* in Germany and *Blue Coat Systems* in the United States. These technologies have been used in authoritarian countries such as Syria, Libya, Bahrain, Tunisia, Iran and Belarus, and it can be assumed that such technologies are used by many other authoritarian regimes as well. This state of affairs is neither in the strategic interests of Europe nor in accord with the goals of a Common Foreign and Security Policy (CFSP) aimed at preventing threats to international security and ensuring non-proliferation. European harmonization of national arms export policies would be necessary here, and this would need to extend to technology systems that are capable of harming the fundamental rights or facilitating the blanket surveillance of Internet users. Existing controls implemented in the EU Code of Conduct and dual-use approval process are as yet insufficient. The *European Parliament* and national parliaments should be comprehensively informed and involved in export decisions. Other sensitive matters are also discussed in secrecy by *European Parliament* and *Bundestag* committees.

Dr. Annegret Bendiek'*s areas of expertise are cybersecurity, Common and Foreign and Security Policy (CFSP), the United States, EU foreign policy, justice and home affairs in the EU, strategic partnerships, and transatlantic relations. She has held a number of research, academic and government positions. Most recently, she was at the German Federal Foreign Office as Policy Planning Staff joining the project "Review 2014 – A Fresh Look At German Foreign Policy" and worked previously as a fellow at the German Marshall Fund for the Transatlantic Academy.*

An Ethical Argument for High-Security IT

by Sandro Gaycken

From an ethical point of view, cyberwarfare is a fascinating new subject that brings together many different issues in security ethics and media ethics in a unique way. In the big picture, it is true that cyberwarfare is still war, or at least conflict, whose fundamental form is not affected by the arrival of the new agents, hackers. The main motives and features of war are largely preserved, conventions such as the law of war do not require any kind of new interpretation, and of course there can also be a just war in cyberwar, with the result that there is no justification for simplistic narratives of a categorical shift, or in calls for a blanket ban.

However, from the ethical perspective, the agency of hackers in conjunction with the particular substrate on which they act, with the equally particular modes of action and resulting tactical conditions and strategic options, is something new. Manipulative observation and action in complete silence and invisibility, or under a false flag, tactical exploitation of information, of knowledge and opinion, or of detailed technical processes buried deep within social systems, and the symphonies of these actions in geostrategic effects, provoke conceptual and operational shifts in many traditional approaches of "offensive" and "defensive", and hence new weightings or new hierarchical configurations of values, which, in turn, require ethical consideration.

Incidentally, not all of this is necessarily negative. Cyberwarfare has an appealing set of characteristics in that it can be conducted in a way which is low-cost, extremely precise and entirely "bloodless". Always militarily desirable, the goal of victory without fighting, even against a superior enemy, has become more possible than ever before through the advent of cyberwarfare. If it is possible simply to put an army out of action during an intervention, so that any further hostile activities are technically impossible, this ability alone may have a significant peace-keeping and stabilizing effect.

However, the goal which is preferred as a matter of military necessity is not necessarily always the ethically preferable one. If the unjust invader can disable the just defender – and not the other way around – then ultimately cyberwarfare appears after all to be just a method and means, rather than a separate type of warfare, and as such it is subject to that duality of any technology according to which it cannot be particularly condemned, nor particularly preferred, without a context. Thus what will be required in future is above all a detailed, technologically and contextually informed description for specific cases – such as the "information operations" variants, which should be regarded as controversial – in which it is possible to decide more specifically under what initial conditions and subject to what circumstances value judgments can be made and considered. Yet from today's perspective, even taking into account a certain degree of progress in the international law debate, this is still a long way off.

Nevertheless, at the present time there are a number of clearer ethical problems, particularly relating to the constant erosion of security and its needlessness. To highlight this erosion and the associated problems more distinctly,

it is necessary to briefly outline the status quo of IT security.

So what is the current risk situation? The cybersecurity problem remains pressing, and is still far from being solved. The likelihood of attacks has hardly decreased. Quite the opposite: There are significantly more attackers, since the NSA has done a good job of advertising in this field over recent years. First there was *Stuxnet*, an impressive demonstration of sabotage capabilities and of an enormous reach and strike efficiency. Then, like an avalanche of advertising brochures for cyberoffensive troops, came the Snowden documents, which demonstrated how extraordinarily much has already happened in this field and – *ex negativo* in the NSA's lack of detection prior to the publication of these documents – how extremely effective camouflage, deception and invisibility are in this area, how easy it is to attack, intercept, manipulate and carry out sabotage in this field.

Consequently, many actors are interested in building up an offensive force. Organized criminal cartels and every intelligence service in the world will now be pushing to acquire such capabilities. In this respect, the risk is increasing.

So is the risk falling in respect of vulnerabilities and damage, as a result of better IT security? Unfortunately not.

At the present time, the foundations of our information technology systems are not becoming more secure, but rather less secure. The fundamental problems of tens of thousands of critical vulnerabilities in our IT substrate have in no way been fixed or even adequately addressed in an innovation strategy. While some companies have made investments, it has hardly been with a strategic direction, or sufficient resources. Other big industry players are actually cutting back. *Microsoft*, for example, recently dissolved its security department, making some staff redundant and moving others into the more lucrative cloud business. From here, therefore, from one of the juggernauts among the *de facto* IT monopolists, no increase in security can be expected. Owing to rapid expansion in many fields, with new flaws and vulnerabilities, a large increase in insecurity is more likely.

The IT security industry, despite a lot of attention, has also not done much. This field is populated by small and medium-sized enterprises with insufficient resources to finance major innovations in anticipation of possibly distant future returns, whose perspective on the problem is still structurally oriented to small-scale cybercrime, as they pursue outmoded development paradigms of the nineties and noughties. These paradigms are evinced in detail in the three lines of attack "defend", "degrade" and "deter".

"Defend", the first line of attack, involves three paradigms "ad hoc", "ex post facto" and the "perimeter" concept, and is concerned primarily with setting up one or more boundaries with observation and intervention options in a sociotechnical system, and with the management of incidents upon detection. Yet detection in this field – and especially in cyberwar, which makes the most efficient use of cybersecurity flaws – is ineffective. The NSA operations, for example, came to light almost entirely via the Snowden documents. Of more than 230 operations which are now known to have existed in 2011, only one was detected (*Flame*). This speaks volumes about the effectiveness of the entire approach. Furthermore, the concepts for incident management are immature and lack strategic focus. They are based on the already weak hypothesis that as a defender you have few advantages, but you at least have the advantage that you know and can better control your own territory. Thus, while accepting that it is not possible to prevent an attack, the aim is at least to prevent the exfiltration of

information by the attacker. However, since attackers have at their disposal numerous options for exfiltration, this concept too is still awaiting proof of its effectiveness. Avoidance of the occurrence of incidents, i.e. an increase in basic passive security, only takes place in rudimentary and helpless form, for instance employee training that warns against opening strange attachments (and conveniently shifts responsibility onto the user). This approach, too, particularly in a cyberwar, owing to the many possible vectors of attack, is practically irrelevant and serves only to guarantee a basic level of hygiene. That which is clearly preferable – the establishment of higher basic resistance – i.e. the *ex ante* unassailability of a system, lies outside the conceptual reach of current approaches to IT security.

"Degrade", the second line of attack, is cited as a complement to "defend", and can be similarly quickly dealt with. Here it is assumed that given good enough detection of attacks, a system with information sharing can be built, via which detected attacks are promptly notified to all potential victims, who consequently arm their own detection mechanisms and are no longer attackable. This in turn is supposed to have the long-term result that attacks are on a significantly smaller scale and are less economically appealing to attackers. Yet this arrangement fails to consider various structural features, such as the poor detection rate already mentioned, and then the high modularizability and easy variability of attacks, the attackers' precise economic models and possibilities for their impairment through "degrade" approaches, the requirements for completeness and operational efficiency of information sharing, the tactical flexibility of attackers in switching to business models which scale in different ways and – again particularly in the case of cyberwar – the equally tactical alternative of scaling not through mass distribution in many different systems, but through targeted, yet persistent, laterally spreading attacks. All these factors raise considerable doubts about the "degrade" approach, which, however, can neither be proved nor disproved, since the necessary empirical data are shrouded in obscurity. But experiences from industry with the years of information sharing and particularly with more dangerous espionage campaigns provide evidence of the failure of this approach, at least in practice.

"Deter", the last line of attack, is finally also conceived of as a complement to the two other approaches. In this case, the traditional active deterrent idea of "deterrence by punishment" comes into play, where attackers are either threatened with drastic measures in the event of successful attribution, or countermeasures are directly imposed on attackers as a punishment intended to impact on the cost/benefit rationale for future attacks. But this approach, too, has had only limited effectiveness to date. Attribution, owing to the inevitable, necessary structural features of being digital, is an unsolvable problem of cybersecurity. Current success stories of attribution, such as the exposure of Chinese espionage campaigns, are merely superficial successes, since they must have received assistance from human intelligence, to a large extent could only have come about due to major flaws in the enemy's operational security, and furthermore are to a certain degree politically supported and desired. Current attempts to establish attribution should therefore be regarded as being only temporary, and they have the further disadvantage of forcing attackers into evolutionary development of better camouflage and operational security. Because of the extensive scope that exists in this respect, these attempts will hardly screen out or deter attackers, but will make the problem significantly more invisible.

Thus none of these approaches brings particularly clear or sustainably effective security gains. Instead, it can be assumed that uncer-

tainties are shifted in various ways, but which have been neither tactically nor strategically anticipated, and which could therefore even produce a series of unpleasant surprises.

The net result of the widespread buildup of offensive capabilities along with an expansion of vulnerabilities, together with paradigmatically inefficient IT security technologies, is an accelerating, spreading and heterogenizing lack of security manifested as an increased possibility of attack, in asymmetrical form, since it is much stronger in states and structures that are highly technologized.

Now, based on this initial situation, a number of particularly problematic points can be identified with regard to security ethics and the ethics of technology. They are described briefly here.

The negligence of tolerating a lack of security

First of all, it may be stated that the lack of security in IT is widely known and in many cases has been known about for a considerable length of time, and it is tolerated to an absurd degree. In many places, over many years and up to the present day, people have worked in certain knowledge of high vulnerability along this vector, especially within many militaries, without the problem being sufficiently escalated politically to initiate lasting change. In part, this tolerance is due to complicity. In the past, many of today's security actors thought that flawed security approaches were sufficient, and implemented those approaches. Now they cannot change their position without raising doubts about their basic competence. Other, new security actors are unable to master the complexity of the topic and tend to delegate or diffuse their responsibility – often to security or IT companies. Tolerance also arises as a result of epistemic uncertainty, ranging from assumptions about the reality of the risk to the relationship between the actual and potential costs of security flaws versus their elimination, to a lack of knowledge about systemic weaknesses in existing security approaches. Both problems give rise to their own ethical perspectives and questions. Tolerance through complicity raises general questions about professional ethics and, in cyberwarfare, the inseparably related special responsibility of the military in its professional role of defender. There is a need to discuss how self-protection of one's career should be weighed up against responsible security conduct, and what alternatives can be developed that facilitate morally less problematic behavior. Other questions are raised by epistemic uncertainty and resultant problems with regard to the ethically preferable behavior in situations with high risk and high uncertainty. In view of the high risk of war and geostrategic erosion present in cyberwarfare, if there is uncertainty regarding the appropriate perspectives on the problem and the levels of protection to be implemented, it might be advisable to adopt a "maximum" approach, i.e. to assume the worst and – provided no significant conflict of values occurs – to implement maximum security requirements. For a more precise evaluation, the difference between acceptance and acceptability as relevant to the ethics of technology, which is emphasized by Christoph Hubig, could be considered here. What is accepted by businesses or militaries based on semi-informed scenario assessments produced at short notice, and on a cybersecurity return on investment that is difficult to estimate, is not necessarily acceptable. Rather, what is acceptable should be formulated first, so as then to be able to address deficits in the practice of acceptance and associated conflicts.

Increase in conflict potentials

Another difficulty associated with the initial situation described above is that the large number of security flaws incentivizes many other military and criminal actors to develop offen-

sive capabilities. Of course, in purely theoretical terms, this may have a neutral overall effect or lead to a positive change in stability, but it is likely to result in a multiplication and heterogenization of the problem, and create problematic offensive path dependencies among the actors, as once capabilities are acquired, their offensive use is at least more likely to suggest itself than before. This too is not necessarily a bad thing, for instance if the offensive use is in the context of a just war. However, the preponderance of unjust war and the numerous possibilities for subversive or tentative warfare resulting from the incentive of high invisibility and falsifiability of identities suggest that multiplication, heterogenization and increasing path dependencies will result in a growing number of smaller conflicts in the special case of cyberwarfare. These in turn could lead to escalations more easily than in other, more strongly established varieties of war, since the novelty of cyberwar means that the interpretation of even minor incidents is still uncertain and, amplified by media hype, could end up being more aggressive.

Escalatory compensation mechanisms

Another problem that arises and needs to be addressed ethically is the compensation mechanisms for poor basic security that become apparent in the "deter" approach. Despite glaring shortcomings in passive protection and the attribution of attacks, these mechanisms still attempt to develop a deterrent effect by drastically increasing the size of the penalty – which is the only thing that still remains in the realm of deterrence. In other words, if it is not possible to stop and only rarely possible to identify an attacker, then the attacker should at least receive a draconian punishment if, for once, he or she is successfully caught, so as still to achieve any kind of deterrent effect at all. While this line of reasoning is militarily functional and understandable (and is already practiced experimentally, e.g. in the Tallinn Manual, at least in the form of harsh threats), it significantly increases the risk of escalation by inviting a corresponding attitude to false flag operations under the particular condition of the falsifiability of identities. At the same time, it gives "honestly caught" attackers the impression of highly disproportionate action, which the accused attacker might then compensate for with other reactions, producing a spiral of escalation. Finally, in the context of compensation mechanisms, there is also the problem of significantly increasing global Internet surveillance, with its very own collateral damage to freedom – since the functioning of "deter" approaches requires maximum efforts to acquire intelligence about the enemy, which can be achieved above all via surveillance technologies.

These three problems are currently three of the more difficult structural problems of cyberwarfare. At the same time, they have clearly identifiable ethical dimensions.

However, in addition to simply weighing up values and determining the methods to be used for this weighing up, any ethical discussion will also require alternative courses of action if it is to have theoretical substance and practical relevance. Here the question arises first of all whether we even possess any alternatives. For if there are no other options, we are simply faced with practical constraints, which may not seem very ethically desirable, and which we may complain about, but about which ultimately there is little to discuss, since there are no alternatives. Particularly in the field of IT security, we do indeed frequently encounter this attitude of surrender to a lack of alternatives. Many of the existing actors are too used to the status quo, and new actors in any case are unaware of any options, with the result that it has almost become an article of faith that we just have to live with this lack of security, like we do with climate change.

But this is wrong.

In many niche areas, the computer sciences have developed various approaches to high-security IT, which is less vulnerable as a basic technology and which by technological means simply does away with a large portion of the cybersecurity problems. In particular, the high number of vulnerabilities resulting from widespread programming errors, and the poor transparency and control resulting from excessive complexity, are serious and fundamental problems that have actually been technically solvable for some time. High-security IT may then be the decisive game-changer that also effectively addresses the three problems discussed above. Firstly, the security gains resulting from high-security IT are so clear-cut, so dramatic and so conclusively demonstrable that they leave no more room for negligent tolerance of security flaws in critical structures. The initial costs are affordable and no performance losses are expected, thus making for an even better and clearer case – especially from the point of view of acceptability. Secondly, the prompt inclusion of high-security systems in critical structures would have the effect of significantly inhibiting the development of the attacker field. Almost all of the smaller actors would no longer be able to muster the resources and expertise necessary to attack such structures, while for bigger actors the cost-benefit calculations would be thrown back to the level of the 1980s. The golden age of signals intelligence would return to a bronze age, and the global conflict potential resulting from high and widespread offensive capacity and escalation would be significantly reduced. Thirdly, there would no longer be any kind of basis for escalatory compensation mechanisms, since there would no longer be a fundamental lack of security needing to be compensated for, or rather since the compensation mechanisms would be a significantly worse option. This would eliminate destabilization due to possible escalations and losses of freedom due to mass surveillance.

High-security IT would therefore be an ethically preferable solution to the cybersecurity problem. The only – but big and powerful – enemy of this approach is the giant that this new approach would kill, namely the old IT. Above all it is the manufacturers and monopolists of existing chips and operating systems, of enterprise resources software and other products, who are preventing the emergence of this specific alternative approach. And thus much in this field ultimately revolves around the question, to be evaluated ethically, of whether we should be supporting a structurally deficient IT substrate at the expense of global security.

Dr. Sandro Gaycken'*s research is focused on privacy, internet freedom, cybersecurity and its impact on modern warfare, intelligence and foreign affairs. He aims to solve the strategic cyberdefense problem through strong high security IT-concepts from computer science, coupled with strong industrial policies to overcome market failures. He is appointed director in NATO's SPS program on national cyberstrategies and director of the cybersecurity working group. He served in the design of the German Foreign and Security Policy on IT-matters as the lead-author of the "internet freedom" and the "cybersecurity/ cyberdefence" parts of this policy. He testified as an expert in many hearings in the Bundestag and provided strategic advice to the UNO, NATO, G8, EU and IAEA. He also served as an expert witness in international court cases concerned with military cyber espionage and cyber sabotage.*

Cyberwarfare: Challenges to International Law

by Robin Geiß

Global networking opens new opportunities for prosperity, education and democratic participation. At the same time, new threat horizons open in cyberspace. Recent years have seen a considerable increase in both the volume and sophistication of cyberattacks. One need only recall the 2007 denial-of-service attacks in Estonia, or the manipulation of Iranian nuclear facilities by *Stuxnet* in 2010. Fueled by a strategic prioritization of military cyber capacities – especially in the United States and China, who are unanimous in classifying cyberspace as a new domain of warfare[1] – these cyberattacks have triggered a controversial debate over the application of international law, notably the right of (military) self-defense in cyberspace and the applicability of the law of war in connection with future cyber conflicts (cyberwarfare).

Meanwhile the question of whether international law – relevant portions of which are based on treaties agreed at a time when the idea of cyberspace was beyond anyone's powers of imagination – is even applicable to events in cyberspace can now be regarded as settled. At least in respect of this initial question, nations today are in agreement: There is no vacuum of (international) law in cyberspace. As hitherto applicable, international law also applies in principle in respect of activities in cyberspace. The greatest challenge, therefore, is to determine how conventional rules of international law can be applied within the special technical structure of cyberspace and how any gaps or loopholes can be closed in a way that serves the legitimate interests of all parties through a dynamic interpretation or if necessary a reform of the existing legal framework. To examine these questions is the aim of this article, which in keeping with the thematic focus of this series of articles limits itself to questions of principle in international law in connection with the military dimension of cyberspace.

The right of self-defense under international law in cyberspace

The international law debate initially focused mainly on cyberattacks which could trigger the right of (military) self-defense enshrined in Article 51 of the UN Charter. Specifically, the issue was when does a cyberattack reach the threshold of an "armed attack" within the meaning of Article 51 of the UN Charter, since it is then – and only then – that self-defense first comes into consideration. Within the bounds of proportionality, however, this could involve a conventional military response. Traditionally, this threshold has been set very high. If the general prohibition of force laid down in the UN Charter is to be upheld, the right of self-defense must remain an absolutely exceptional right. This must also and particularly apply to any cyberattacks. Only if a cyberattack produces consequences which in their extent and severity are comparable to those of a conventional armed attack can it be assumed that such an attack would trigger the right of self-defense. Technical experts agree that a cyberattack can indeed reach this high threshold, for instance if industrial facilities or air traffic control and other traffic guidance systems are manipulated and actually cause death and destruction. The NATO countries recently confirmed their agreement with this opinion in their cyber

defense policy of June 2014.[2] So far, however, none of the cyberattacks which have become publicly known have reached the threshold of such an attack. This is true even of the *Stuxnet* attack in 2010, which, of all the cyberattacks that have become known so far, probably came closest to the attack threshold in view of its physical impacts on the Iranian nuclear program. A further issue of particular controversy is whether a cyberattack on *Wall Street* or the *Frankfurt Stock Exchange* might not also reach the threshold of an attack that triggers the right of self-defense. One reason that it might is that any such cyberattack could have devastating consequences. However, according to conventional interpretations there is agreement that economically damaging acts do not constitute an "armed attack" within the meaning of Article 51 of the UN Charter. This does not mean that a country has to stand by and watch such events take place. Even below the "armed attack" threshold, international law permits countermeasures as a response to internationally wrongful acts, depending on the severity of the attack. Nor is it entirely out of the question that international law in this area will change in the future, for example if countries were to decide that in globally networked financial and economic systems, the economic harm caused by acts such as cyberattacks could reach a completely new and potentially existential level of threat. So far, however, there has been no indication of any such change in opinion among the international community.

Yet aside from the threshold discussion, the technical characteristics of cyberspace offer another reason why, in many cases, an invocation of the right of self-defense does not come into consideration: Self-defense always requires clear identification of the attacker. The International Court of Justice in The Hague has expressly prohibited self-defense where there is no clearly defined adversary. But in cyberspace it is often extremely difficult to sufficiently identify the attacker and produce the required evidence. At any rate during the limited window of opportunity constituting the only time when self-defense against an armed attack comes into question, this will often prove impossible. The possibilities for concealing or manipulating the origins of an attack in the virtual realm appear to be virtually unlimited, especially for militarily experienced countries.

Military cyber operations in the context of (future) armed conflicts

Apart from the discussion concerning the right of self-defense, another focus of debate is whether International Humanitarian Law is capable of adequately containing military cyber operations in future armed conflicts in keeping with its humanitarian objectives. With regard to certain types of military cyber operations, the International Humanitarian Law assessment is already clear. If a cyberattack is launched against a clearly identified, purely military target – e.g. a cyberattack which seeks to disable a military command center – there are no international humanitarian law concerns. According to applicable international law, such acts are legal in the context of an armed conflict. It is equally clear, for example, that malicious software which spreads in an uncontrolled fashion akin to a biological weapon, causing damage to civilian as well as military facilities, is unequivocally prohibited. On the whole, most scenarios will be covered by applicable international law in which, like the air in an aerial attack, cyberspace is ultimately used only as a medium for carrying out an attack against a physical target. At any rate, such scenarios do not raise any fundamentally new issues.

In contrast, it would appear much more difficult to assess the legal situation when components (hardware and software) of cyber

infrastructure are themselves to be made into a strategic target. To the extent that countries are developing their capacities to wage war in cyberspace, this scenario is becoming increasingly relevant. A considerable and worrying legal gray area still exists here.

The networked structure of cyberspace makes it more difficult to apply the principle of distinction which is fundamental to International Humanitarian Law. This principle states that in an armed conflict, a distinction must always be made between military (attackable) objectives and civilians (who are protected from direct attack). In the globally networked realm of cyberspace, it may not be possible to uphold this principle, and there is a danger that all manner of cyber infrastructure components could be far too easily deemed targets for military attack. This would turn the logic of International Humanitarian Law on its head. The problem here is that under current law, any object used for military purposes in an armed conflict is in principle considered to be a legitimate target for attack for the duration of its military use. While the number of such "dual-use" objects (i.e. civilian objects that can be used for military purposes) was limited in traditional conflicts, the situation in cyberspace is different. Worldwide civilian cyber infrastructure is not only potentially suited to civilian and military use, it is already used on a large scale (simultaneously) for military purposes.[3] In the event of an armed conflict, this could lead technologically advanced countries in particular to follow an interpretation which affords the greatest possible scope for action and intervention – also in military respects. In view of the enormous hunger for data on the part of the National Security Agency (NSA) – even in peacetime – this fear appears to be in no way unfounded. European countries should take a clearer stance than they have done thus far in support of a narrow interpretation.

Furthermore, in view of the extensive interconnectedness of cyberspace, military attacks on key components of cyber infrastructure could have far-reaching and unpredictable impacts on civilians and civilian applications. The International Committee of the Red Cross has insistently drawn attention to this issue.[4] Since the NATO states in their Wales Summit Declaration have just recently acknowledged that cyberattacks will become more sophisticated, common and potentially damaging in the future,[5] in this respect too a more thorough investigation of the problem at national level would seem appropriate, and a clear positioning desirable with regard to the application and interpretation of the principle of proportionality under international humanitarian law – which sets an important limit on impacts on the civilian population – in cyberspace. The U.S. Department of State recently issued some initial proposals in this regard which are a step in the right direction.[6]

Conclusion

To sum up: The right of self-defense exists in cyberspace too. In view of the considerable evidential difficulties in the virtual realm, the greatest restraint should be exercised in any future invocation of this right in connection with cyberattacks. In the field of International Humanitarian Law, there are many issues requiring clarification in connection with potential impacts on the civilian population, which could be particularly serious in countries where economic and social life are reliant to an ever greater degree on a functioning cyberspace. The debate must therefore advance beyond the mere declaration that cyberspace is not a vacuum of international law.

Finally it should be pointed out that the virtual realm presents many other potential threats aside from the military dimension, which are only gradually receiving more attention (in the context of international law). In particular, this

applies to the threat to privacy and freedom of expression which has become apparent in connection with the NSA affair, as a result of the merging of traditional intelligence activities with the mass surveillance of private citizens, but also in respect of industrial espionage and the broad spectrum of cybercrime. While the discussion of the military dimension of cyberspace is a forward-looking debate, which in the absence of any corresponding (discernible) established practice among states is based in part on speculation about military capabilities in cyberspace, mass surveillance, industrial espionage and cybercrime are already no longer hypothetical but extremely real threat scenarios.

1 See e.g. The Economist, War in the Fifth Domain, July 1, 2010, available at: http://www.economist.com/node/16478792.

2 NATO, Wales Summit Declaration, September 4-5, 2014, margin nos. 72 et seq., available at: http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

3 U.S. Department of State, International Law in Cyberspace, September 18, 2012, available at: http://www.state.gov/s/l/releases/remarks/197924.htm.

4 ICRC, What limits does the law of war impose on cyber-attacks?, June 28, 2013, available at: http://www.state.gov/s/l/releases/remarks/197924.htmhttps://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm.

5 NATO, Wales Summit Declaration, September 4-5, 2014, margin nos. 72 et seq., available at: http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

6 U.S. Department of State, International Law in Cyberspace, September 18, 2012, available at: http://www.state.gov/s/l/releases/remarks/197924.htm.

Prof. Dr. Robin Geiß *is Professor of International Law and Security at the University of Glasgow and head of the research project "Charting the International Legal Framework for Security Governance by external Actors in Areas of Limited Statehood" in Berlin. Previously he was Professor of International and European Law at the University of Potsdam and worked as a UN delegate and legal adviser to the "International Committee of the Red Cross" (ICRC) in Geneva and New York. He is managing editor of the "Yearbook of International Humanitarian Law" and rapporteur of the International Law Association's study group on the challenges of asymmetrical armed conflicts. He was also a member of the international group of experts that drafted the "Tallinn Manual" on cyberwarfare at the NATO "Cooperative Cyber Defence Centre of Excellence" (CCDCOE) in Tallinn.*

State-Sponsored Hacktivism and the Advent of "Soft War"

by George R. Lucas, Jr.

Not so long ago, cyber "activism" (on the Internet, at least) was limited to pranks, practical jokes, and random acts of vandalism. Pranksters attached software "viruses" to emails that, when mistakenly opened, quickly spread through your organization's internal network, posting goofy messages and perhaps even erasing data on your hard drive. Cybervandals posted offensive messages or unwanted photos, or otherwise defaced your organization's website for no apparent reason. About the only crimes committed in those early days were trespassing (technically, by "invading" your private company network or your computer itself) and destruction of property. Apart from mean-spiritedness or a perverted sense of humor, however, about the only reasons given for such malicious activities were a collective grousing by disaffected programmers and computer "geeks" about the monopolistic practices, and mediocre software distributed by *Microsoft Corporation*.

Malicious behavior in the cyberdomain, however, quickly evolved into a variety of more serious and sinister activities. On the one hand, it was not long before sophisticated individuals and criminal gangs exploited the very same software vulnerabilities as pranksters, but did so in order to steal your bank deposits, credit card numbers, or even your personal identity. On the other hand, cyber "activism" itself likewise evolved into ever more sophisticated acts of political sabotage: defacing or even temporarily shutting down government or commercial websites with so-called "DDoS" attacks (distributed denial of service), dispatching software "worms" that traveled from computer to computer, penetrating each machine's firewall and virus protection software in order to gain control over the PC's or laptops themselves, transforming each into a "zombie." These individual machines were then remotely networked with others into a massive "botnet" controlled by political dissidents or criminal organizations, who, in turn, used them to launch DDoS attacks on banks and financial institutions and divert their funds to secret accounts.

"Hacktivism" is a term that came into somewhat indiscriminate use to classify all these distinctive and diverse acts of malevolence and mischief in the cyberdomain, ranging from straightforward crime and vandalism, to many forms of political protest carried out on the internet. Technically, the "hacktivist" is one who engages in vandalism and even in criminal activities in pursuit of political goals or objectives, rather than simply for personal satisfaction or financial gain. Well known individuals (like Julian Assange of *WikiLeaks*) and loosely-organized groups like *Anonymous*, *LulzSec*, and *Cyberwarriors for Freedom* resort to internet malevolence to publicize their concerns, or otherwise further their political aims. These concerns range from personal privacy, liberty, and freedom of expression to opposition to political regimes like Syria or Egypt.

In February 2014, Dr. Mariarosaria Taddeo of the University of Warwick, president of the International Association for Computing and Philosophy, organized an international workshop, sponsored by the *UNESCO Committee on Cyber Security*, in order to examine the ethical dimensions of hacktivism, as well as the chal-

lenges posed by the exponential increase in this form of cybermalevolence[1]. During those discussions, I described three distinct ways of being a hacktivist, symbolized in turn by the activities of *WikiLeaks*, the behavior of individual agents in the cyberdomain (like former NSA contractor Edward Snowden), and groups like *Anonymous*.

The three concerns I cited as motivations for each were, in the same order: transparency, whistle-blowing, and vigilantism. *WikiLeaks* purports, for example to provide greater transparency regarding the otherwise covert activities of government and large corporate organizations. The actions of whistle-blowers (like U.S. Army Private Bradley (Chelsea) Manning, and NSA Contractor Edward Snowden) aimed specifically to expose what each individual took to be grave acts of wrong-doing or injustice on the part of the U.S. government or military (in these specific cases). The internet vigilante group *Anonymous*, by contrast, is a bit harder to pin down, since the loosely organized federation's individual members espouse a wide variety of disparate causes. The organization's behavior in response to each chosen cause, however, clearly involves taking the law (or, in its absence, morality) into the group's hands unilaterally. That is, based upon their shared judgments regarding immoral or illegal behavior by individuals, organizations, or governments to whom the group objects, the group launches attacks against selected targets ranging from the Syrian government of Bashir al Assad (for engaging in massive human rights violations), to organizations and individuals who might be engaged in perfectly legitimate security and defense operations to which members of Anonymous nevertheless object.

This is vigilantism. And, as its name suggests, the members of *Anonymous* cannot easily be traced or held accountable for their actions. As in all instances of conventional vigilantism, the vigilante's judgment as to what or who constitutes a moral offense is deeply subjective, and often wildly inconsistent or otherwise open to serious question. Importantly, in all cases involving transparency, whistle-blowing and vigilantism, the burden of proof is on those who deliberately violate fiduciary duties and contractual (legal) agreements into which they may have entered, or who disobey or flout the law itself, in order to expose or protest against activities they deem to be even more egregious than their own actions. This comparative judgment on the part of the protestor or whistle-blower is technically known as "the Principle of Proportionality." It demands of them that the degree of harm brought about through their own actions be demonstrably less than the harm already done by others to which they seek to call attention, or bring to a stop. The problem is that this comparative judgment is notoriously difficult to make. Vigilantes often exaggerate or misrepresent the harm against which they protest, and seriously underestimate the effects of their own activities on public welfare.

Otherwise, the remaining difficulty with such actions is that there is no independent or adversarial review of these decisions. According to what is likewise termed the "Principle of Publicity" or the "Principle of Legitimate Authority", the final authority to evaluate the legitimacy of the protestor's or dissident's actions rest not with that individual, but with the wider general public, in whose collective interest the individual purports to act. So, in all these cases, it must be possible in principle to bring the individual dissident's actions and intentions before an impartial "Court of Public Opinion" for independent review. The last criterion is the one most frequently ignored, and most often failed by both vigilantes and would-be whistle-blowers. They are prone to suffer from an abundance of self-righteousness.

The Advent of State-Sponsored Internet Activism

Having established this context for the discussion of cyberhacktivism generally, what now are we to make of its most recent evolution: namely, the rise of state-sponsored or government "hacktivism?" Nations and governments are entering the cyberfray alongside private groups, either attempting to combat or shut down other hacktivists and stifle dissent within their own borders, or instead, to pursue political objectives against other states that were traditionally resolved through diplomacy, economic sanctions, and finally, a resort to kinetic force. Many states at present appear to be resorting to massive cyberattacks instead. Such nations are thought to include pro-government groups or organizations in China (e.g., *Shanghai Unit 61384* of the People's Liberation Army), the Russian Federation, and especially North Korea. The "Russian Business Network", a branch of organized crime in the Russian Federation, is believed to have cooperated with the government in launching a preemptive cyberattack on government organizations and military sites in the Republic of Georgia in 2008, prior to a conventional Russian military incursion into the breakaway Georgian province of Ossetia. The U.S. recently indicted five members of the *Shanghai unit 61384* by name, for having been responsible for massive thefts of patents and trade secrets from U.S.-based aerospace and defense industries. The indictments were not expected to result in actual arrest and prosecution, but were intended instead to send a message to the Chinese government that its disavowal or denial of state accountability for these crimes under international law was no longer plausible.

One of the most interesting new developments is the work of *Cyber Fighters of Izz ad-Din al-Qassam*, an organization that takes its name from a prominent early 20th-century Muslim cleric and anti-colonialist. In 2012, on the anniversary of the 9/11 terrorist attacks in the U.S., this group allegedly carried out a massive DDoS attack on U.S. financial institutions. The attack was described in a *Twitter* post by the group as having been launched in retaliation for the continued presence on *YouTube* of the American-made film, "The Innocence of Muslims," which portrays Islam and the prophet Mohammed in a very scandalous and unflattering light. The group vowed to continue the attacks until the offending film itself was removed from the Internet.

Two things stood out regarding the resulting, very serious disruptions of American financial institutions. First, despite its claim of independence, the group's attack was not indiscriminate. The institutions targeted were primarily those that had complied with the terms of the ongoing U.S. economic sanctions against Iran. In particular, the group's demand that a film be censored on account of its political or religious content seemed hollow: their leaders had to know that this was a demand that was beyond the power of a democratic government anywhere to grant.

The second oddity was that the anonymous *Twitter* site from which this group issued its September 2012 proclamation turned out to be the same account from which messages had flowed a few weeks earlier (allegedly from another vigilante group entirely) in the aftermath of a massive cyberattack on the internal computer network of *ARAMCO*, the Saudi Arabian oil giant. Those attacks, on 15 August 2012, allegedly carried out by an organization calling itself the *Cutting Sword of Justice*, erased data on all affected computer drives, and inserted in their place the image of a burning American flag. U.S. security officials seemed quite certain that the first of these attacks was an act of retaliation by Iranian agents in response to the damage done to their own nuclear and oil infrastructure by *Stuxnet* and *Flame*, respectively, both weapons attributed to (but

never acknowledged by) the U.S. and Israeli governments.

Suppose all these allegations and counter allegations are true: in particular, suppose that the two attacks in close sequence in 2012 (and others since) were not carried out by distinct and independent organizations, but instead represent the coordinated actions of a state government (Iran), retaliating for similar attacks upon its cyberinfrastructure by other states (Israel and the U.S.). Add to these the known and ongoing, state-sponsored, malevolent cyberactivities of the People's Liberation Army in China, the "Russian Business Network", and North Korean operatives. The conclusion is that states, as well as individuals and dissident groups, are now directly and deeply involved in hostile activities that increasingly transcend the boundaries of traditional espionage, covert action, and the "dirty tricks" of the past. Rather, this ongoing, high-stakes, but low-intensity conflict carried out by states against one another has evolved into what several colleagues (e.g., Michal L. Gross, of the University of Haifa) are coming to call "soft war."

Cyberhacktivism and "Soft War"

By analogy with the concept of "soft power," "soft war" is a mode of warfare or conflict that is intentionally non-kinetic: i.e., it does not entail the use of conventional weapons, or the destruction that accompanies conventional armed attacks. But it is still a very grave matter. Real damage is done, and real harm is inflicted, although rarely (save in the case of *Stuxnet*) does this involve physical harm to physical objects. Rather, the conflict results in loss of information, loss of access to information processing, and an inability to carry out essential activities (such as banking, mining, medical care, trade, and commerce) that rely largely upon information processing.

Unlike the highly-publicized concept of a "cyberwar," however, the weapons and tactics of "soft war" are not limited to the cyberdomain. They can involve state use of the media, including cyber social media as well as conventional media, for purposes of propaganda, confusion, obfuscation, and disinformation. Soft war could involve the use of non-lethal (or "less-lethal") weapons in conventional attacks. For terrorist "pseudo-state" groups like *Hamas*, it could involve using civilian volunteers as "human shields" to deter conventional attacks on physical infrastructure or military installations by adversaries, one among a range of non-violent tactics termed "lawfare," using the law itself (in this instance, the Law of Armed Conflict) to thwart an adversary.

The evolution of cyberconflict itself toward the "soft war" model of hacktivism, specifically, is quite different than the full-scale, effects-based equivalent of cyber "warfare" predicted by many pundits (such as Richard Clarke) during the last decade. The much-touted "cyber Armageddon," or "cyber Pearl Harbor" was to be a massive disruption and destruction of conventional systems, like air traffic control and electrical grids, resulting in widespread death and destruction on parallel with a massive conventional war. But state-sponsored vigilantism and hacktivism appear to signal something quite distinct from this familiar, but often highly exaggerated and implausible scenario. This state-sponsored conflict is virtual, not physical; non-violent, rather than kinetic; but nevertheless quite destructive and malevolent in other respects, equally capable of causing massive social upheaval, or bringing about a "death by 1,000 cuts" through pilfering of industrial and state secrets, or by interference in trade, commerce, finance, medical care, and transportation.

And, just as with increased reliance on the exercise of "soft power" (diplomacy, sanctions, media relations and the like), the advent of "soft war" has distinct advantages for those nations that engage in it. Essentially, this kind

of warfare substitutes cleverness and ingenuity for brute strength. It is less costly to wage, less destructive of property, of lives, and of national treasure (as well as international prestige). Yet it is quite capable of achieving the same political goals, when properly utilized, as "hard" kinetic war, as well as capable of undermining or fending off an adversary that relies solely upon "hard" war tactics. It is, in short, the equivalent of bringing Asian martial arts that rely on balance, timing, and tactical sophistication to bear upon an enormous, powerful, but wholly conventional bully. The martial arts expert can hold his or her own, and even prevail, even though smaller, lighter, and perhaps less physically strong than the bully.

This comparison is apt, since "soft war" is directly attributable to two Chinese military strategists, reflecting on the future of military conflict in the aftermath of the lopsided victory of U.S.-led coalition forces in the 1991 Gulf War against the conventional forces of Iraqi President Saddam Hussein. In a landmark essay in 1999 entitled "Unrestricted Warfare," two senior colonels in the People's Liberation Army, Qiao Liang and Wang Xiangsui, argued that the U.S. had become an international bully, physically too strong and too reliant on extensive war-fighting technology to resist by conventional means. Instead, they proposed, new forms of conflict needed to be devised, more indebted to subtleness and cleverness than to brute force, in the spirit of Sun-Tzu, in order to effectively oppose the brute physical power of the American "hegemon."

There is no explicit regime under international law that specifically governs this kind of conflict. Ought there to be? Or is it sufficient to rely on state interests, and the norms emergent from accepted state practice, to serve as a guide for when, and for how, to engage in "soft war?" Ought the same or similar guidelines applicable to kinetic war also guide entry into and conduct during this "soft" mode of warfare as well? Or ought it to remain, as its original formulators speculated, "unrestricted" or "without bounds?"

Might we not reasonably require, for example, that states only engage in such conflict when presented with irreconcilable differences sufficiently grave to justify conventional use of force (as, admittedly, happened on both sides of the Iran/U.S.-Israel dispute over Iran's nuclear weapons program)? And, as that example suggests, ought we to demand or reasonably expect that, when faced with the alternative of resorting to "soft" or kinetic warfare to resolve such disputes, that (consistent with a "Principle of Last Resort"), not only should all viable and reasonable alternatives short of war be attempted, but that the "soft war" alternative should always be chosen in lieu of the conventional resort to the use of kinetic force? Perhaps most importantly, might we demand, or reasonably expect, that nations engaging in such conflict with one another should do their utmost to avoid deliberate targeting of purely civilian, non-combatant individuals and their property, as is legally required in conventional war? Or, as in the example of using volunteer civilians as human shields, should attacks on financial institutions or civil infrastructure that merely involve a denial of access or service be subject to a more tolerant regime in which the combatant-noncombatant distinction is less viable, and perhaps less significant?

"Soft War" and "Soft Law"

These are the questions waiting to be addressed and clarified in the wake of the advent of "soft war" generally, and specifically in the aftermath of the increased resort by state-sponsored agents to the kinds of tactics once limited to dissident individuals or non-state groups. While the lion's share of such normative work has occurred within the context of existing international law (most notably, the Tallinn Manual of 2012), I myself have begun

to believe that the legal framework will simply not suffice to provide reliable guidance in this new domain of conflict. There are a number of reasons for this skepticism.

Contributors to the Tallinn Manual, for example, including some of the most eminent legal minds in the world today, brilliantly attempted to interpret and extrapolate existing international law (the regimes pertaining to armed conflict and humanitarian treatment of war's victims, and those pertaining to criminal activity in particular) so as to bring existing legislation to bear upon conflict in the cyberdomain. But as I have described above, "soft war" is not "war," strictly speaking. Neither is it crime (although it sometimes involves the commission of otherwise-criminal actions by state agents). Finally, "soft war" includes, but is not limited to the cyberdomain. "Media war" is not "war," and it is also not limited to cyberconflict. Use of non-lethal weapons, or tactics of "lawfare" (including human shields) not only occur outside the cyberdomain (and so are obviously not addressed in the Tallinn Manual), but (in the latter instance) are also designed precisely to frustrate the bright-line statutes of existing international law, turning the letter of the law against its underlying regulatory purpose.

Even in the cyberdomain alone, "soft war" tactics there are more akin to espionage than to war or crime, and are not explicitly addressed in international law, nor are state parties to existing legal arrangements eager to see such matters addressed there. In fact, this is the chief obstacle to pursuing normative guidance through the medium of law: those who are party to the law, and whose consent would be required to extend or amend it, are deeply opposed in principle to any further intrusion upon their respective interests and activities through treaty or additional legislation. Insofar as international law rests fundamentally upon what states themselves do, or tolerate being done, this opposition to further legislation (the one issue in the cyberdomain on which the U.S., Russia, and China seem to agree) seems a formidable obstacle to pursing governance and guidance through legal means. [The recent and spectacular failure of the Tallinn Manual to achieve widespread international acceptance or anything resembling U.N. endorsement beyond its NATO-country constituents provides an instructive case in point.]

This is not as unpromising as it might seem, however, when one recognizes the historical fact that the principle bodies of international law pertaining to conflict of any sort largely codify, after the fact, norms of certain kinds of practice that emerge from public reflection by the practitioners themselves upon the better and worse features of that practice, and upon the ends or goals ultimately served by these practices. Law and regulations give the appearance of being stipulative, and are thought to be imposed externally, often upon unwilling subjects or agents. Best practices, by contrast, emerge from the shared practices of the interested parties, and reflect their shared experience and shared objectives.

International law, seen in this light, is more properly understood as grounded in common accord, consensus, and voluntary compliance. Its inherently cosmopolitan character (often overlooked by politically-appointed "Committees of Eminent Persons," eager to impose their terms of behavior on others) instead reflects Immanuel Kant's conception of standards of regulative order that moral agents themselves have both formulated and voluntarily imposed upon themselves, in order to guide and regulate their shared pursuits. Their compliance with principles that they themselves have formulated is thus more feasible and readily attainable.

This is a somewhat prolix manner of expressing a doctrine known in international relations as "emergent norms." This concept is encoun-

tered more broadly in moral philosophy as a kind of "trial and error," experiential groping toward order and equilibrium, a process that Aristotle (its main theorist) described generally as the methodology of the "imperfect" sciences. The great contemporary moral philosopher, Alasdair MacIntyre, is chiefly credited with having resurrected this methodology in the modern era, from whence we can discern it already at work in the cyberdomain, as well as in the field of military robotics [as I have demonstrated extensively elsewhere in my formal publications on these topics.] Legal scholars, for their part, have dubbed this sort of informal and voluntary regulatory institution (as occurs in the Codes of Conduct of professional organizations, or the deliberations and recommendations of practitioners in the aftermath of a profound moral crisis) as constituting "soft law".

What is required at the moment, it seems to me, is a coherent and discernable body of "soft law" for "soft war." That is, the relevant stakeholders in the community of practice – in this case, frankly, adversaries engaged in the kind of low-intensity conflict that I have described under the heading of "soft war" – to formulate and publicize the principles that they have evolved to govern their practice. In earlier eras, like the Cold War, for example, espionage agents from adversarial nations evolved a sophisticated set of norms to govern their interaction and competition, designed largely to minimize unnecessary destruction, loss of lives in their respective clandestine services, mutual treatment of adversaries in captivity and prisoner exchanges, and other tactics designed to reduce the risk of accidental or unnecessary escalation of conflict (especially conflict that might cross the threshold of kinetic war in the nuclear era). All of these informal normative arrangements intended to facilitate, rather than inhibit, the principle aim or goal of espionage itself: reliable knowledge of the intentions and capabilities of the adversary. In the nature of things, there were no "councils" or "summit meetings," and no published or publicized "codes of conduct." Rather, these norms of prudent governance and guidance came to be "understood" and largely accepted (and complied with) by the members of this interesting community of practice.

What the broad outlines of the content of this "soft law" for "soft war" might be are already outlined above, utilizing somewhat more familiar "just war" terminology, which serves well for this purpose. Adversaries and stakeholders pursuing "soft war" have an interest, for example, in seeing that it does not accidentally "go kinetic," or involve needless and unnecessary "collateral damage" to vital civilian infrastructure, especially of the sort that might lead to widespread physical destruction and loss of life. They share a common interest in proportionate response, and the dictates of military necessity, of the kind exhibited in the conflicts (allegedly) between the cyberwarriors of Iran, the U.S., and Israel described above. And adversaries like the U.S., China, and the Russian Federation, still locked into a preliminary mode of "unrestricted" or limitless warfare, need to consult more directly and frankly than has been possible to date on where common interests lie in imposing boundaries and regulative order on their "soft" conflicts, before the incessant damage being done on an ongoing basis to all parties to these conflicts forces an escalation into something far more serious and irreparable.

On a positive note, this increased resort to "soft war" tactics, including cyberconflict, holds promise that the very real conflicts and disagreements that have often led nations to make war upon one another may themselves evolve into a mode of authentic opposition and conflict resolution that nonetheless ends up resulting in dramatically reduced bodily

harm and loss of life, while doing less damage – and more easily reversible or repairable damage – to the property of adversaries and innocents than was heretofore conceivable in conventional conflict.

1 http://www2.warwick.ac.uk/fac/soc/pais/research/ierg/cyberethics/

George R. Lucas, Jr. *recently retired as Distinguished Chair of Ethics at the U.S. Naval Academy (Annapolis, MD) and is also Professor Emeritus of Ethics & Public Policy at the U.S. Naval Postgraduate School (Monterey CA). Currently, he is visiting guest professor at the Reilly Center for Science, Technology and Values at Notre Dame University (South Bend, IN). His most recent book is "Military Ethics: What Everyone Needs to Know" (Oxford University Press, 2015), and he is the editor of the "Routledge Handbook of Military Ethics" (2015). He is President of the "International Society for Military Ethics" (ISME), and newly-appointed director of the multi-institutional "Consortium on Emerging Technologies, Military Operations, and National Security" (CETMONS).*

Cyberwarfare: Hype or New Threat?

by Götz Neuneck

Recent years have witnessed phenomenal hype surrounding the idea of cyberwarfare, fueled by high-profile cyberattacks on large companies, banks and governments, and the media's frequent use of the term. Countries, too, are increasingly encountering cyberattacks. Spectacular attacks on Estonia, Georgia, Iran and Saudi Arabia have been politically motivated. Consequently, the topic has become the subject of international debate and government planning. After all, states and their governments are themselves increasingly employing cyber techniques, whether for surveillance or espionage, communication or optimizing the deployment of armed forces. Today's weapon systems are networked and rely on digital technologies, engendering the debate surrounding the development, procurement and use of semi-automated armed drones. Such unmanned systems are only controllable if they have data connections, computer systems and ground stations. They are just as much a part of cyberspace as many other civilian and military systems. The Pentagon now refers to cyberspace as a "new domain of warfare". For governments, armed forces, and society at large, this raises the question of how to promote peaceful use of the cybersphere, defend against future threats, and establish effective democratic control.

Western societies have long advocated an "open, secure and peaceful Internet", at the same time as Western militaries prepare for electronic combat in cyberspace. Given constant technological advancement, new military applications and uses of military force will always produce ethical, international law, and security challenges for individual soldiers and for the community of states. Under what conditions are cyberattacks permissible? What is an appropriate response to a cyberattack? How can we protect ourselves against these attacks? What principles of International Humanitarian Law are applicable, and where are provisions lacking? It first needs to be established whether such a thing as cyberwarfare will actually happen in the future, and what the possible implications are for militaries and societies. Then we need to examine whether current international agreements are sufficient for limiting a cyberwar, and what specific responsibilities this entails for societies, governments, militaries and individual users.

Several mutually overlapping debates are concerned, in part, with the future of the "global, free and open" Internet, also in view of efforts by individual states to gain control over national and global infrastructure ("Internet governance"). There is also a fear that the Internet could increasingly be used for militarily motivated cyberattacks. In the event of war, attacks could be directed not only against traditional military targets, but also against private and public infrastructure, bringing modern life to a standstill. If communication infrastructure such as the Internet or electricity supply is out of action for any length of time, key social functions are interrupted, putting a sustained burden on any modern society. Thirdly, militaries might not only conduct hostilities in the Internet, for example, but also respond to cyberattacks with conven-

tional tools of war, and attack vital elements of cyberspace by "kinetic means".

What is cyberwarfare? Can war be fought in the Internet?

Cyberwarfare is understood to mean a coordinated cyber offensive by one country on the government or civilian information networks of an enemy country, with intent to disrupt, disable or destroy their computer systems or information networks. The prefix "cyber" (derived from the Greek term steering), however, is today used rather imprecisely in a wide variety of domains encompassing messaging, the Internet and telephone networks. Cyberattacks, i.e. gaining illegal access to third-party computer systems for the purpose of data surveillance, manipulation or data theft, are now an everyday occurrence in the Internet. Targets are often large companies, but also include military networks and governments. Since every user has access to the Internet, it is often unclear who is behind the attacks and what their motives are. Damage is often limited and purely economic. Malicious software, used to block Internet sites or steal data, is generally accessible. Attack routines are becoming more complex, for instance deploying botnets to launch coordinated remote-controlled attacks via compromised computers in different countries. In 2007, non-intrusive denial-of-service (DOS) attacks shut down bank and government online services in Estonia. Cyberattacks today are also byproducts of real conflicts, such as in the Ukraine or Syria, where websites of parties involved in the conflict are attacked. Meanwhile more complex, intrusive attacks by viruses or trojans can cause substantially greater damage, especially if they affect critical infrastructure such as the electricity supply or financial system.

Indications of cyber offensive tools

The discovery of *Stuxnet* in 2010 marked the first known time that malicious software had been successfully used to conduct cyber sabotage, when a combination of spyware and controller malware was used to infiltrate the controversial uranium enrichment plant in Natanz, Iran, and directly destroy several hundred centrifuges. It would be fair to call the *Stuxnet* worm the first digital, targeted "cyber weapon". Cyber offensive tools consist of program codes that gain access to a logical or physical environment and have the capability to disable or destroy real objects. It is not known whether usable cyber weapons in fact already exist, but there are indications that cyber offensive weapons are being developed in a few countries, notably the United States. In 2012, the Pentagon research agency DARPA invited tenders for the "Foundational Cyberwarfare (Plan X)" project, which sets out to research "innovative approaches" to cyberwarfare. The Pentagon's Defense Science Board in 2013 advocated forming a legion of "cyber warriors" and developing "world class cyber offensive capabilities". The Snowden revelations also brought to light a secret NSA department that had been conducting "tailored attacks" against Chinese IT systems for 15 years. Presidential Policy Directive 20 (PPD-20), signed by U.S. President Obama on October 20, 2012, is extremely telling. It calls upon the relevant agencies to develop "offensive cyber effect operations" (OCEO) and draw up a list of potential targets. Other countries will not wait idly as such developments take place. The likelihood of a cyber tools arms race is mounting along with the number of cases of cyberespionage attempting to spy out possible attack options, such as the U.S. has long accused China of perpetrating.

Ambivalent security measures

A study by the United Nations Institute for Disarmament Research (UNIDIR) in Geneva shows that many countries are setting up and including cyber commands in their regular armed forces and national defense; 114

nations had established cyber protection programs in 2012. The number almost doubled compared with 2011. Purely civilian programs exist in 67 countries, while 47 states give their militaries an additional role and include forms of cyberwarfare in their military planning and organization. So far only six nations have published military cyber strategies. According to media reports, 17 countries state that they are developing "offensive capabilities". For the most part, however, it remains unclear what this means in detail. Overall, there is a lack of transparency regarding the respective fields of application and capabilities. Shedding more light on the various activities is an urgent task for international diplomacy.

Cyberwarfare certainly differs from conventional warfare in important respects. Computer software codes used as a cyber weapon generally exploit vulnerabilities in enemy computer systems or networks. Deep technological insights are therefore an essential requirement here. It takes a certain amount of time to launch a defensive response to a bits and bytes offensive. Moreover, the impact of cyber weapons is non-lethal in the first instance. In view of the complexity of the technology, it is difficult to predict what the potential damage might be. A cascade of collateral effects could occur, as could unintended consequences. Anonymity in the worldwide web makes attribution for an attack harder or impossible. The infrastructure of the Internet is mostly operated by businesses, including multinational Internet providers, meaning that governments do not have any direct access. Furthermore, disruptive cyber tools are "one-shot weapons", whose effects are easily limited by suitable countermeasures once they become known. At the same time, however, attacks on critical infrastructure can cause particularly serious harm. In terms of a strategic cyberwar, there are two conceivable scenarios. One is that in a crisis situation, a country under attack could itself launch a cyber offensive and so escalate the crisis. Alternatively, following a heavy, protracted cyber offensive, a country might retaliate with "kinetic weapons" and so start a conventional war. It is conceivable that in the future, real combat action will be accompanied with cyberattacks on media and also against the enemy military, and furthermore that states are already preparing for such scenarios.

International efforts to regulate cyberwarfare

Western countries such as the United States and the EU regard the most important part of the global cybersphere – the Internet – as a global *res communis omnium* (like the high seas and space) and an economic resource that should remain "free, secure and open" for users. Against this political background and in view of the pace of technological change in both the civilian and the military cyber sector, international and regional organizations and groups of nations have initiated conferences, dialogs and studies on how to improve global cybersecurity. NATO too has picked up on the cyber theme and begun to develop a cyber defense capability, which it is coordinating among its member countries. Its Strategic Concept 2010 talks about cyberattacks potentially reaching "a threshold that threatens national and Euro-Atlantic prosperity, security and stability". It does not set out a clear position on the question of how the alliance would respond to a cyberattack. At the invitation of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, an international group of lawyers was asked to examine whether and how international legal norms and practices are applicable to cyberwarfare. The results were published in March 2013 as the Tallinn Manual. Containing 95 rules, each with a commentary, it reaches the conclusion that cyberspace is not a legal vacuum, that the UN Charter applies to cyber-to-cyberattacks,

and that states are responsible for cyber infrastructure and activities originating from it on their territory. With regard to the prohibition of the use of force laid down in Article 2 (4) of the UN Charter, Rule 10 states: "A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful". It follows from this that a state under attack can exercise its right of self-defense under Art. 51. Accordingly, an extensive cyberattack could very well lead to a conventional war. The exact criteria for when a cyber operation reaches the threshold of an "armed attack" depend on the individual case. Espionage or data theft that result in an interruption to non-existential cyber services can be ruled out. Since there are no exact criteria for determining when the "armed attack" threshold is exceeded in cyberspace, there is a danger of preventive military action being legitimized by the side under attack, and of kinetic attacks against cyber targets becoming "wageable". Nevertheless, the Tallinn Manual provides an interesting basis for further discussion of the applicability of international law to activities in cyberspace. At UN level, in June 2013 a fifteen-strong Group of Governmental Experts (GGE) presented a report to the UN Secretary-General which calls for actions in four categories to promote a "peaceful, secure, open and cooperative ICT environment." The experts suggest that greater consideration should be given to norms, rules and principles governing the responsible behavior of states, based on existing international law, and that "confidence-building measures" (CBMs) should continue to be developed, which can help to prevent further escalation in a crisis. The report contains a list of possible CBMs that could serve as a basis for international agreements. These range from exchanging information about national cyber strategies to establishing regional consultation mechanisms and mutual reporting of cyber incidents. A new UN expert group is currently continuing this work, as are regional organizations such as the Organization for Security and Cooperation in Europe (OSCE). In December 2013, the OSCE Ministerial Council adopted an initial list of CBMs which the OSCE participating states voluntarily commit to implementing. These range from exchanging national views on ICT security, to increased cooperation and consultation, to developing a joint terminology. Individual states have now also initiated bilateral consultations and "cyber dialogs," for example between the United States, Germany, Japan and Russia, while the U.S. and Russia have now set up a kind of "red telephone" to warn each other about cyber incidents.

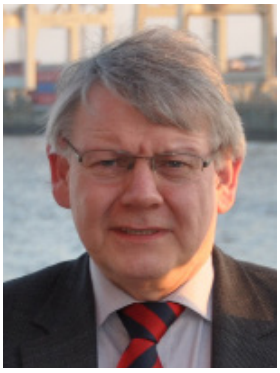
Despite these useful efforts, so far there is still no generally accepted definition in international law of terms such as "cyber offensive weapon" or "strategic cyberwar", or any agreed system of damage classification or effective protection concepts for the cyber realm. Strict limits should be imposed on the eavesdropping activities by intelligence services for which the technical capabilities now exist. Beyond bilateral agreements, there would appear to be an urgent need to strengthen international law with provisions for data protection and the protection of privacy. Criteria and new instruments are necessary to prevent blanket mass surveillance. Industrial espionage should be prohibited, as should mass storage of data for long periods of time regardless of any suspicion of wrongdoing. Parliaments and international organizations, not intelligence services, are responsible for establishing such principles. A single set of rules should be established within the European Union to give EU citizens the right to view data and facilitate its deletion. The computer industry should be required to enhance cyber security and create greater transparency about the data it uses. Users need more information about cyber

security and better training in how to use technology safely. For a timely early warning and more effective crisis management, the relevant authorities, key Internet service providers and research institutes should jointly develop technologies and procedures for better analysis and detection of attack patterns and better defense. Joint exercises and sharing data from forensic analyses are just as important here as mutual technical assistance, regularly sharing experience, and joint table-top or expert exercises by concerned states. It should also be examined whether confidence-building control mechanisms for verification, such as have been tried and tested in the military field, are transferrable. Above all else, the task for international cybersecurity policy is to prevent a digital arms race. During the Cold War era, "confidence and security building measures" (CSBMs) and arms control were important instruments that served at least to prevent an "accidental war" or excessive rivalry in armaments. The establishment of a "red telephone" between the United States and Russia is encouraging. It should set an example for similar efforts between these states and the EU. The agenda at UN level should include the development of principles and instruments of responsible conduct as well as the first CBMs. The OSCE has already adopted an initial list of CBMs to promote transparency, stability and predictability among participating states with regard to the use of information and communication technologies. A first step is the voluntary exchange of national perspectives on national and transnational threats, and on the respective roles of government organizations, strategies and programs. Within the framework of the OSCE, such a process can be fleshed out and become more firmly established through regular meetings of national experts. It would be useful if a database was available for OSCE participating states to record national cyber policies and their respective actors. In subsequent confidence-building steps, the OSCE states could provide each other with details of their respective military cyber components, visit each other's cyber defense centers and conduct joint exercises in this area. In the longer term, agreement on conventions to contain military cyberattacks is advisable.

1 Theresa Hitchens, James Lewis, Götz Neuneck (eds.): The Cyber Index. International Security Trend and Realities, United Nations Publications, New York and Geneva/Switzerland, UNIDIR/2013/3, http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

2 Michael N. Schmitt (ed.): Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge 2013.

3 UN General Assembly, Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security A/68/98, June 24, 2013.



Prof. Dr. Götz Neuneck *is Deputy Director of the "Institute for Peace Research and Security Policy" (IFSH) at the University of Hamburg and head of the "Interdisciplinary Research Group on Disarmament, Arms Control and Risk Technologies" (IFAR²). After completing a degree in physics and gaining his doctorate in mathematics, he worked extensively at the Max Planck Society in Starnberg on interactions between security policy, strategy, and technology. He is a council member of the "Pugwash Conferences on Science and World Affairs", spokesman of the Physics and Disarmament working group of the "Deutsche Physikalische Gesellschaft" (DPG), and representative for the Amaldi Conference of the "Union of the German Academies of Sciences and Humanities". His current work focuses on cybersecurity, new technologies of warfare, and non-proliferation.*

Why Should We Worry About the Militarization of Cyberspace?

by Dinah PoKempner[1]

As a lawyer, and especially as one for a non-governmental international human rights group, I often encounter a good deal of skepticism from some military audiences, who perceive my "mission" as a form of "lawfare," that is, using law as a weapon against state interests. It seemed wise to just flush this out at the start, because it is a misperception with serious consequences for a democratic society and its armed forces, just as downplaying terrorism or insurgency as a threat to human rights is a dangerous game for civil rights advocates. National security and human rights, though often in tension, are codependent in any society in which we would choose to live. Even if we understand national security as a relative, not absolute condition, it is integral to the conception of state obligation to protection of individual rights. The state cannot effectively protect rights if national security and public order are inadequately maintained; one only needs to look to the phenomenon of "failed states" or indeed, to almost any zone of conflict for illustration.

Few dispute that national security and human rights coexist in relation, but the nature of that relationship is under constant debate. Since 9/11, the debate has been heated in counter-terrorism strategy, and well predating Edward Snowden's revelations, it has been heated in the context of digital technology and the regulation of what we imprecisely call "cyberspace" as well. Recently, the rallying cry has been against "militarization of cyberspace," a concern that (perhaps counter-intuitively) shows a good deal of common ground between those whose mission is to defend rights and those whose mission is to defend the nation.

The denomination of these malicious events as cyberattacks in the sense of threats to national security, and the delegation of responsibility (and enormous resources) for preparedness, defense and reaction to military organs, is to a large degree responsible for the perception of militarization. Viewing the cyberspace as an incipient battleground has led to tremendous emphasis on both intelligence and the question of how the laws of armed conflict might apply.

But while there is scholarly debate on what actually constitutes an "attack" in cyberterms, there is a fair amount of consensus that for the purposes of determining what triggers armed conflict or constitutes an act regulated by International Humanitarian Law (IHL), such "attacks" are only a very small subset of the most destructive malicious actions or interventions in cyberspace. A much larger set of what are casually called "attacks" involve economic damage, defacement, espionage, identity theft, reputational damage, or other consequences that are subject to ordinary peacetime law. In terms of established law, these malicious events take place either in armed conflict or its absence, and not in some new and unregulated dimension. Human rights, both through the vector of municipal and international law, apply regardless, except to the extent modified in armed conflict by the *lex specialis* of IHL, or the limitations or derogations permitted under various human rights laws and treaties.

To sketch the legal territory is not to say any of the demarcations or applications are clear, or there is no need for further law. Indeed, it's quite muddy out there, with the boundaries between a state of armed conflict and the absence of armed conflict hazy and subject to fluctuation, cyberattacks frequently transnational but with weak means of international protection and regulation, and deterrence or retribution complicated by problems of attribution. Great struggles involving states, their militaries, industry, civil society and technologists are still in progress over whose code will predominate in what situation and what standards ultimately govern the Internet. But as novel as we think "cyberspace" and its features may be, it is dangerous to conceive of it as *terra nullius*, an empty land where self-help is the rule. For one thing, we are living there; our communications, economies, relational networks, defense systems, culture, and our human rights are all situated in this medium on which we grow more dependent by the day. The legal landscape may be a bit foggy, a bit wild, but we should not think it is foggy in the sense of the "Fog of War", where a margin of overreaction, miscalculation or error is accepted, or wild in the sense of the Wild West, where the gun is the law.

To begin with, the condition of war is not the default setting of a democratic society. With good reason the law questions prolonged declarations of emergency; these are often hallmarks of the undemocratic societies or ones that have settled into permanent abrogation of rights. The absence of armed conflict is not necessarily "peaceful"– it can be full of insecurity, ongoing threats and attacks, both internal and external – but it also is not simply the pause between wars. In a democratic state, the power of response to threats and attacks in peacetime is given to authorities subject to constant public and political accountability, through oversight, rule-making and adjudication. This produces a much different mindset than a single-minded focus on military preparedness.

The state's deployment of force in peacetime, even in exigent situations, is highly regulated by concepts of human rights that are alien to the battlefield. It is well accepted, for example, that even in a public emergency, law enforcement officers must use force as a last resort and in a way so as to minimize damage and injury – even to the criminal suspect. Longstanding international standards for law enforcement require that lethal force only be used for the purpose of protecting life. To lawfully incapacitate someone in peacetime requires not simply capture, injury or destruction – where these acts are permitted at all – but also authority deriving from a particular law criminalizing particular intentional behavior. Then, even assuming the state has got a plausible criminal suspect in hand, that person is entitled to a presumption of innocence and can contest the state's action and win, unless the state provides the requisite amount of proof in a fair and usually public trial before an independent judiciary with full rights of due process and defense. Given this burden, public officials in peacetime really don't have broad license for mistake or overreaction, and consequently don't like to operate too much in a gray zone where it could be difficult to sufficiently justify their actions and win their cases. We accept these less than optimal conditions for protection of security because we do not want to live in a police state, where our liberties would constantly be subordinated.

Of course, the greater the apparent threat to the nation's security, the more likely it becomes that democratic polities will loosen restraints and allow greater latitude and powers to the state, sometimes edging nearer or even sliding into the legal regime governing conflict. The recent paradigm for this is the so-called "war on terror" in the United States, which

was accompanied by greatly expanded police powers, limitations on rights, and a legislative authorization for the use of military force that was interpreted expansively to enable military action far from the theatre of battle in Afghanistan, and is now being repurposed to justify intervention against the *Islamic State in Syria and Iraq*. It has been observed that it is easier to understand the beginning point of armed conflict than the point at which it ends, and this is true even beyond issues of direct military engagement. Once the nation is invested in armed conflict, inevitably this condition influences its peacetime institutions. A rebound effect from resort to military force can be seen in municipalities across the United States, who often employ veterans of war in law enforcement or corrections, and who receive Pentagon surplus weapons that are often unnecessary and inappropriate for keeping the peace in a civilian society. The heavy-handed approach of the police to protest in Ferguson, Missouri, had at least some roots in these practices.

These intangible effects of the different mindset and standards of armed conflict are part of the reason why it is important to be sensitive to the nuances of terms like "attack," a gateway term between the laws of armed conflict and peacetime law. In the sense of *jus ad bellum*, there has been a good deal of scholarly debate as to what type of cyberoperation would constitute an "armed attack" under Article 51 of the UN Charter sufficient to permit self-defense and override Article 2(4)'s prohibition against "the threat or use of force against the territorial integrity or political independence" of another state. Most writers point to the severity and purpose of the anticipated consequence, such as whether the cyberattack has similar effects to a kinetic attack (lives lost, planes or trains crashing). Target may also matter, such as an attack bent on disabling a state's critical infrastructure or its military operations. Attribution of the attack to a state rather than a criminal gang (when that can be determined) may be relevant, as well as duration of the attack, and whether it is related to contemporaneous kinetic attacks. But even this rough list should demonstrate that a cyberattack justifying the use of force in national self-defense is a relatively rare event. The pervasive discourse of "cyberattack" and "cyberwar" in policy circles to refer to the whole world of malicious actions obscures this and undermines thinking on robust peacetime protections.

Similarly, the standards of IHL that regulate state response in "attack" revolve around anticipated military advantage. Whatever this means – for it is also a contested concept – it is not the same as the objectives of law enforcement, which center squarely on the protection of human life and security (which, it must be noted, is not the same thing as the elimination of all threat). While in practical terms proportionality governs the use of force in both law enforcement and IHL situations, the difference in objectives makes for profoundly different calculations, means, methods and outcomes.

"National security" is a similar term, pivotal in international human rights law as signaling points of limitation or derogation of certain rights. Though undefined in human rights instruments, it has been given contours through adjudication and commentary in both national and international fora. To begin with the most extreme national security case, a number of international human rights instruments allow derogation of certain rights in a declared public emergency which threatens the life of the nation. This might include some situations of armed conflict or natural catastrophe, but not necessarily all, and even then the measures taken must be strictly required by the exigency of the situation and no longer than necessary. If ordinary limitations will suffice to handle the situation, derogation is unacceptable, and in any event, many rights

are non-derogable. Thus strictly limited in scope and duration, derogation is hardly the wholesale suspension of human rights law, which continues to apply even in situations of armed conflict. So the term "national security" is neither a light switch that "turns on" the military framework of IHL, nor one that automatically "turns off" human rights.

Apart from these extreme and temporary situations, some rights may be limited in the ordinary course of events to protect national security, provided such limitation is actually necessary and no more intrusive on the right than needed to handle the threat in a democratic society. It is difficult to imagine, for example, a necessary and proportionate protection of national security requiring either suspension or restriction of privacy of correspondence on a massive scale because of endemic threats such as crime or terrorism, although targeted and temporary intrusions on privacy may be justifiable.

To appreciate the application of this principle, it is vital to hold "national security" to the meaning it has in human rights law, rather than in political rhetoric. While not a specifically defined treaty term, it has evolved through usage by international bodies, courts and scholarship to entail protection of the state's existence, territorial integrity or political independence from threat or use of force, as well as preservation of the state's capacity to respond to such a threat. Courts and international interpretive bodies have rejected equating diplomatic embarrassment, threat to the current government, or economic disadvantage to a threat to national security. But right there the gap between existing law and politics is evident, as officials have defended surveillance as necessary for economic or geopolitical advantage, or for being able to search large groups – perhaps even whole countries – for indicators of incipient radicalization apart from any specific situation, all purposes international human rights law would not recognize as necessary to protect national security.

While many scholars complain of the difficulty of governing war by law, the project of regulating surveillance or other state cyberoperations is at least as fraught. Surveillance of individuals can be lawful, but is usually secret and even when detected or suspected, not very susceptible to challenge in court due to doctrines of standing, state secrets, deference to national security concerns, etc. When conducted on targets outside the state's territory, it is usually illegal in the foreign state's law, but seldom exposed or prosecuted even when detected. Freedom of information regimes, and even parliamentary inquiries, often run into the wall of secrecy too, and in the cases where surveillance orders are evaluated or approved by courts, these proceedings or decisions may be undisclosed as well. Unfortunately, invoking national security to reflexively avoid public review of surveillance hollows out the concept of legality over time. Reliance on law that has no tether to democratic accountability risks losing public trust and confidence in the legitimacy of the state's actions and policies. This encourages on the one hand, vigilantism, as in the appeal to victims of retaliatory "hackbacks," and on the other hand, retaliation against the state (or against companies seen as its agents or facilitators). Neither is conducive to securing genuine national security much less avoiding cyberwar or protecting human rights.

What, then, is conducive to these goals, which must also be goals for military leaders in any democratic society? In 2013, a UN group of governmental experts with China, Russia, the United States and the United Kingdom as long-standing members, managed to agree that "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful

and accessible ICT [Information and Communications Technology] environment." It further concluded that "State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments". This in itself is a strong affirmation that we are neither in the Wild West nor in some foggy new dimension. Yet while there are clear landmark principles of international law to follow, there is much to be done in elaborating them and making them applicable to cyberevents.

First, recognizing that the vast majority of malicious events in cyberspace are not "attacks" in any sense of *jus ad bellum* or *jus in bello*, we should stop talking as though they were. That means applying normal criminal law and civilian authority to their investigation, prosecution and adjudication. When the U.S. treated terrorism as "war," even when it was unrelated to actual armed conflict, it led to grave violations of fundamental rights and legal principles, degraded the U.S.' soft power, and created terrible precedents for the transborder use of force. One hopes that these mistakes will not be replicated in the domain of cyberspace. To that end, it is unhelpful to characterize protests, or even protests with some incidentally damaging element, such as some under the *Anonymous* umbrella, either as "attacks" or "terrorism" when what they amount to is essentially the cyberequivalent of defacement of property or symbolic, evanescent or nuisance-grade civil disobedience, in the tradition of chaining oneself to the gates of the nuclear plant.

Similarly, when considering cybercrime, it is important to apply normal principles of law and not use the term "national security" as a trump to human rights interests. Not every conceivable threat to an interest of the state or its government of the day implicates national security. Publishers who reveal the leaks of whistleblowers may embarrass a government or make its diplomacy more complicated, but without tangible evidence that they have damaged the territorial integrity, political independence or defense capability of a state, their rights and the rights of their readers should not be abridged. Where whistleblowers reveal secrets, the actual damage to national security, in the sense that human rights law gives that term, should be put in the balance against the considerable interest in speech and the public's right to know of official wrongdoing, an aspect of access to information that is in some situations termed "the right to truth." Even where national security is plainly under threat, that fact must not short-circuit public, legislative and judicial review of preventative measures that compromise rights. There is already an evolving body of cybercrime law that addresses a wide array of public interests. While not all emerging cybercrime laws are well-considered or balanced in terms of rights protection, in democratic societies they are generally subject to the normal legal and political processes that test framing, interpretation and application, and this testing process is best when it fully engages the public and civil society.

With respect to ensuring that a peacetime framework governs most state actions relating to national security in cyberspace, it is critical to consider the separation of military and civilian direction of cyberpolicy at the national level. Indeed, at the close of 2013, the Review Group on Intelligence and Communications Technology recommended to President Obama the appointment of a civilian head of the National Security Agency, but the White House declined to adopt the view of its own hand-picked advisors. While there is no doubt that coordination is needed between civilian and military agencies of government in the area of intelligence as well as territorial security and defense,

there are important reasons why these functions are separate in most democracies. It is unhealthy for the military to serve a political agenda rather than a nation. Civilian agencies, in contrast, are headed by political appointees and responsible for implementing policies and laws created by politically accountable officials. It's not bad that the NSA has created a senior risk assessment position to "look at the big picture", but when the functions of signals intelligence gathering and offensive cyberoperations share a roof with a mission to defend critical infrastructure, there are bound to be conflicts of interest that one or two positions, however senior, will find difficult to reconcile. This is the sort of issue that requires broad government engagement, and not just in one or more executive departments.

The conflation of military and civilian authority in some countries mirrors the entanglement of civilian and military infrastructure in cyberspace. The reliance of military cyberoperations on civilian infrastructure and civilian companies has troubling implications for the principle of distinction in the event of armed conflict. U.S. multinational companies that long avoided locating customer data in countries known for human rights violations now face increasing pressure to localize because of the U.S. government's invasion of such data, with and without these companies knowledge. Without shared protocols and commitment to protect rather than exploit civilian infrastructure, we can expect that such infrastructure will become a fair target; a predicament that in turn feeds militarization of approach to cyberthreats. International action is needed, both to segregate critical civilian infrastructure and mark it in ways that create strong presumptions of illegality of attack. This sort of segregation and marking may be difficult, and may always be imperfect and incomplete, but without efforts and experiments in feasibility, the principle of distinction will be extremely difficult to implement in cyberspace.

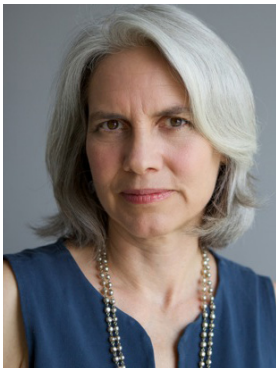
The dangerous game of trying to find a gray zone without rules is being played out with the question of whether civilian data is a protected object under the laws of war. The Tallinn Manual, a comprehensive study of the application of international humanitarian law applied to cyberwar, recognizes cyberinfrastructure and hardware as potentially a civilian object, but denies that status to data and code, under the rational that it is intangible. This conclusion, which rests on an old commentary of the International Committee of the Red Cross (ICRC) parsing the analogue world of military objectives as visible, tangible "objects," would render the deliberate targeting of civilian databanks as outside IHL unless it affected some physical computer system as well. So you could not target a civilian data bank were it written on paper, but you could aim to destroy it if it were written in code. Various commentators have noted this is hardly a plain or intuitive reading of the law as applied to a new means of war, and it is squarely at odds with the purpose of IHL to protect civilians from the effects of armed conflict. The dangers of enabling no-holds barred attack on civilian data should be obvious, and of deep concern to everyone.

Finally, the feasibility of arms control should be firmly brought onto the international agenda in all its dimensions, including verification and confidence building measures. This has already begun with discussions of the need to regulate particularly dangerous surveillance technology being sold to highly abusive governments by European firms. The European Commission, in a report this April to the European Council and Parliament, recognized "the emergence of specific 'cybertools' for mass surveillance, monitoring, tracking and interception" and noted "cyber-proliferation" as an important dimension of export controls. The issue is also coming to the attention of national

governments, particularly as remote interception products made by Western companies such as *Gamma Group* and *Hacking Team* turn up in countries with a solid record of repression, being deployed against "threats" such as human rights activists and political protestors.

There are already many discussions on such topics, but most exclude civil society apart from the occasional academic or the ICRC. Experts on cybersecurity such as Ronald Deibert have called for "civil networks to be players in rule-making forums," a mandate he puts into creative practice at gatherings of policy makers, technical experts, academics and activists. Multistakeholder engagement including technicians, corporations, and academics is becoming more accepted as a mode in many areas of cyberpolicy but in matters of cybersecurity, the vital role of human rights experts who can speak to both war and peacetime contexts is sometimes overlooked. This is a critical dimension of the international law governing cyberspace, and the ethical considerations that democratic societies employ to define themselves and defend their security. Partnership between the military and the human rights movement, both experts in human security, is essential to preventing cyberspace from becoming a prospective battlefield and keeping it a realm of democratic society.

1 General Counsel, Human Rights Watch. The author would like to thank Camille Francois, Cynthia Wong and Eileen Donahoe for their insights and suggestions; errors, however, are her own.



Dinah PoKempner *is general counsel of Human Rights Watch. As a field researcher, she documented torture, war crimes, and other serious violations of international human rights and humanitarian law in Vietnam, Cambodia, North Korea, China, and former Yugoslavia. At Human Rights Watch, she is currently responsible for the development of institutional positions on international law and policy and ethics of human rights practice. Her writing encompasses freedom of expression, cyber freedom, privacy, hate speech and defamation of religions, whistleblowing, peace-keeping operations, international tribunals, U.N. human rights mechanisms, humanitarian law and refugee issues, and the development of the human rights movement. She is a graduate of Yale University and Columbia University Law School.*

What Ethics Has To Do With the Regulation of Cyberwarfare

by Mariarosaria Taddeo

Since the first cyber-attack to Estonian websites in 2008, the debate surrounding the regulation of cyberwarfare has grown fast and has accompanied concrete efforts to understand whether and how existing international laws and treaties could be endorsed to regulate it. Such efforts have proven to be quite demanding and were not the exclusive concern of the military; they have also had a bearing on ethicists and policy-makers, since existing ethical theories of war and national and international regulations struggle to address the novelties of this phenomenon.

In the rest of this article I will analyse how some of the most relevant tenets of Just War Theory (JTW), and the international laws and treaties implementing them, are applied to the case of cyberwarfare. In doing so I will also focus on the interpretations of existing laws and regulations given in the so-called Tallinn Manual.[1] This has been the first and, so far, the most exhaustive work devoted to offer guidance in their application to the case of cyberwarfare. The manual offers a valuable contribution to the debate over the regulation of cyberwarfare, for it shows that extant laws and treaties can be stretched to address this phenomenon and that when it comes to the international ground, the cybersphere is not a new Wild West. However, while very interesting and important, this approach inevitably finds its own limit as it overlooks the conceptual roots, i.e. JWT, on which laws regulating cyberwarfare rest. In doing so, it misses the possibility of truly expanding the scope of existing laws by reshaping their conceptual framework. The consequence is that the approach fails to consider and to account for the conceptual changes prompted by cyberwarfare and risks confusing an *ad hoc* remedy with the long-term solution, and, in the long run, risks imposing conceptual limitations on the laws and regulation for this new form of warfare.

A fully satisfactory regulation of cyberwarfare requires to take into account the novel scenario determined by the dissemination of the information revolution, which in turn demands an in-depth revision of our understanding of key concepts such as those of violence, attack, and warfare. Without such understanding the application of existing laws and treaties to cyberwarfare will remain a stretch, which will eventually reach its limits and generate a regulatory vacuum. To overcome the latter, a theoretical effort is needed to design new norms and principles that will allow for its regulation not by stretching an old blanket but by properly and adequately addressing the novelty of this phenomenon. Before focusing in more details on CW, let me alert the reader that the rest of this article is devoted to highlight the problem at stake but not its solution, which requires far more philosophical work than I could do in the space of this article.[2]

The ontological hiatus

I shall refer to cyberwarfare as to "[…] the use of ICTs [Information and Communications Technology] within an offensive or defensive military strategy endorsed by a [political authority] and aimed at the immediate disruption or control of the enemy's resources,

and which is waged within the informational environment, with agents and targets ranging across the physical and non-physical domains and whose level of violence may vary upon circumstances".[3]

Two aspects of cyberwarfare are noteworthy here: the informational nature and its transversality with respect to the sets of targets, the domains in which it is waged and its levels of violence. The transversality of cyberwarfare it is better appreciated once it is considered within the framework of the so-called information revolution,[4] which has a wide impact on many of our daily practices: from our social and professional lives to our interactions with the environment that surrounds us. With the information revolution we have witnessed a shift, which has brought the non-physical domain to the fore and made it as important and valuable as the physical one. Furthermore, physical and non-physical are fully merged and integrated to the point that any distinction between the two domains is imperceptible.

Cyberwarfare is one of the most compelling instances of such a shift. It shows that there is a new environment, where physical and non-physical entities coexist and are equally valuable, and in which states have to prove their authority and new modes of warfare are being specifically developed for this purpose. The shift towards the non-physical domain provides the ground for the transversality of cyberwarfare. This is the aspect that most differentiates it from traditional warfare and is also the feature that engenders the ethical and regulatory problems posed by cyberwarfare. In fact, while it is accepted as uncontroversial that the disruptive (non-kinetic) outcomes of cyberwarfare can inflict serious damage to contemporary information societies and at that CW may also lead to highly violent and destructive consequences – dangerous for both military forces and civil society, there is much less agreement on the moral value of the intangible objects that are targeted in the non-kinetic cases of cyberwarfare.

The confusion rests on an anthropocentric approach to the understanding of cyberwarfare, in which moral value is only ascribed to living and physical things. As cyberwarfare involves informational infrastructures, computer systems and databases, it brings new objects, some of which are intangible, into the moral discourse. Therefore, there is a hiatus between the ontology of the entities involved in traditional warfare and those involved in cyberwarfare and between the entities considered by JWT and those involved in cyberwarfare. Such a hiatus affects the ethical analysis cyberwarfare and subsequently its regulation. As it has been described by Randall R. Dipert, "[s]ince cyber-warfare is by its very nature information warfare, an ontology of cyber-warfare would necessarily include [a] way of specifying information objects […], the disruption and the corruption of data and the nature and the properties of malware. […] A cyber-warfare ontology would also go beyond […] a military ontology, such as agents, intentional actions, unintended effects, organizations, artefacts, commands, attacks and so on" (see endnote 2).

The first step towards an ethical regulation of cyberwarfare is to determine the moral status of such (informational) objects and their rights, lest incur in the problems highlighted in the next session.

Regulating Cyberwarfare

When it comes to regulating warfare, JWT offers the most refined and complete conceptual framework and there is little doubt that just war principles and their preservation hold in the case of traditional warfare as well as in the case of cyberwarfare. Nevertheless, it would be mistaken to consider JWT both the necessary and sufficient ethical framework for the regulation of cyberwarfare, since address-

ing this new form of warfare solely on the basis of JWT generates more ethical conundrums than it solves.

The problems arise because JWT mainly focuses on the use of force in international contexts and surmises sanguinary and violent warfare occurring in the physical domain. As the cyber domain is virtual and cyberwarfare mainly involves abstract entities, the application of JWT becomes less direct and intuitive.

The struggle encountered when applying JWT to the cases of cyberwarfare becomes more evident if one considers how pivotal concepts such as, e.g. the ones of harm, target, attack have been reshaped by the dissemination of this new type of warfare. See for example Dipert, who argues that any moral analysis of this kind of warfare needs to be able to account for a notion of harm "[focusing] away from strictly injury to human beings and physical objects toward a notion of the (mal-)functioning of information systems, and the other systems (economic, communication, industrial production) that depend on them".

The definition of what counts as an attack or as a use of force in cyberwarfare and what, as such, can trigger the waging of a war or a conflict is not less problematic than the one of harm. In this respect it is quite useful to compare two definitions, the one provided by the National Research Council in its 2009 report on cyberattack capabilities (Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities 2014), and the one offered in the Tallinn Manual. In the former, a cyberattack is defined as "the use if deliberate actions – perhaps over an extended period of time – to alter, disrupt deceive, degrade or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks" (p. 80).

The Tallinn Manual defines cyberattacks as "a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" (see endnote 1, p. 106). The National Research Council's definition offers a more specific characterisation of cyberattacks, including non-physical damages as well as physical ones, while the scope of the definition offered by the Tallinn Manual remains undecided, for it depends on the definition of 'objects'. If these are understood as physical objects, then the manual is by default considering as attacks only kinetic uses of cyber technologies. This seems actually to be the case if one considers the focus of the definition on physical damages and the absence of any reference to damages to intangible objects, e.g. data, information, and informational infrastructure.

The consequences of such an approach are extremely relevant for they affect the application of *jus ad bellum* as well as of *jus in bello*. For example, rule 10 of the Tallinn Manual stresses that under *jus ad bellum* a cyberattack is unlawful if it constitutes a threat or use of force against a state. Rule 11 refines Rule 10 by stressing that a cyberattack amounts to a use of force if its scale and effects are similar to those of non-cyber-operations. Criteria based on the magnitude and effects of a cyberattack have been proposed to assess if the former amounts to a use of force or to an armed attack, like the one described in Rule 11 of the Tallinn Manual. All this is quite uncontroversial, for a cyberattack that has the same or similar effects to a conventional attack should be treated as a kinetic attack in the eye of the law.

Still, cyberwarfare includes informational infrastructures, computer systems, and databases. In doing so, it brings new intangible objects into the moral discourse. The moral status of such (informational) objects and

their rights need also to be ascertained when designing norms regulating cyberwarfare. The risk is otherwise to compromise the application of JWT to the case of cyberwarfare, this is the case for example of the principle of "more good than harm".

According to this principle, before declaring war a state must consider the universal goods expected to follow from the decision to wage war, against the universal evils expected to result, namely the casualties that the war is likely to produce. The state is justified in declaring war only when the goods are proportional to the evils. This is a fine balance, which is somehow straightforwardly assessed in the case of traditional warfare, where evil is mainly considered in terms of casualties and physical damage that may result from a war. The equilibrium between the goods and the evils becomes more problematic to calculate when considering cyberwarfare.

If strictly applied to the non-kinetic instances of cyberwarfare, the principle of more good than harm leads to problematic consequences. For it may be argued that, since cyberwarfare can lead to victory over the enemy without incurring casualties, it is a kind of warfare (or at least its non-kinetic instances) that is always morally justified, as the good to be achieved will always be greater than the evil that could potentially be caused.

Nonetheless, cyberwarfare may result in unethical actions – destroying a database with rare and important historical information, for example. If the only criteria for the assessment of harm in warfare scenarios remain the consideration of the physical damage caused by war, then an unwelcome consequence follows, for all the non-violent cases of cyberwarfare comply by default to this principle. Therefore, destroying a digital resource containing important records is deemed to be an ethical action *tout court*, as it does not constitute physical damage per se.

The problem that arose with the application of this principle to the case of cyberwarfare does not concern the validity per se of the principles. It is rather the framework in which the principles have been provided that becomes problematic. In this case, it is not the prescription that the goods should be greater than the harm in order to justify the decision to conduct a war, but rather the set of criteria endorsed to assess the good and the harm that shows its inadequacy when considering cyberwarfare.

Conclusion

In concluding this article, I shall leave the reader with three fundamental questions that need to be answered to overcome the problems described in this contribution:

1. The first question revolves around the identification of the moral agents, for it is unclear whether an artificial agent, like a virus, should be considered moral agents, or whether this role should be attributed to the designer or to the agency that deployed the virus.
2. The second question focuses on moral patients. The issue arises as to whether a computer system should be considered the moral receiver of the action, or whether the computer system and its users should be considered the moral patients.
3. Finally, the third question concerns the rights that should be defended in the case of a cyberattack. In this case, the problem is whether any right should be attributed to the informational infrastructures or to the system compounded by the informational infrastructure and the users.

The issue addressed in this paper is not whether the case of cyberwarfare can be considered in such a way as to fit the parameters of kinetic warfare and hence to fall within the

domain of JWT, as we know it. This result is easily achieved if the focus is restricted to physical damage and tangible objects. The problem lays at a deeper level and questions the very conceptual framework on which JWT rests and its ability to satisfactory and fairly accommodate the changes brought to the fore by the information revolution, which are affecting not only the way we wage warfare, but also the way in which we conduct our lives, perceive ourselves and the very concepts of harm, warfare, property, and state.

It would be misleading to consider the problems described in this article as reasons for dismissing JWT when regulating cyberwarfare, or for discarding altogether existing laws and regulations of warfare. Instead, the problems described in this article point to the need to consider more carefully the case of cyberwarfare, and to take into account its peculiarities, so that an adequate conceptual framework will be developed to properly take into account "contemporary values" while developing laws to regulate cyberwarfare.

1 NATO Cooperative Cyber Defence Centre of Excellence. 2013. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge; New York: Cambridge University Press.

2 The reader who wishes to know more about ethical analyses of cyberwarfare may read Dipert, R. 2010. "The Ethics of Cyberwarfare." Journal of Military Ethics 9 (4): 384–410; Taddeo, M. 2014. "Just Information Warfare", Topoi, forthcoming; Taddeo, M. & Floridi, L. 2014. "The Ethics of Information Warfare", Philosophy of Law, Comparative Law, International and European Law Series, Springer.

3 Taddeo, M. 2012. "Information Warfare: a Philosophical Perspective", Philosophy and Technology, 25.1, 105-120, p. 112.

4 Floridi, L., 2014. "The Fourth Revolution – How the infosphere is reshaping human reality", Oxford University Press.

Dr. Mariarosaria Taddeo *(University of Warwick and Oxford) focuses on the ethical analysis of cybersecurity practices and information conflicts, philosophy and ethics of information. She published several papers on online trust, cybersecurity and cyberwarfare and guest-edited a number of special issues on the same topics. She also edited (with L. Floridi) a volume on "The Ethics of Information Warfare" (Springer, 2014) and is the author of "The Ethics of Cyber Conflicts" under contract for Routledge. She is the 2010 recipient of the Simon Award and of the 2013 World Technology Award for Ethics. She serves as an associate editor of Philosophy & Technology and is the president of the International Association of Computing and Philosophy.*

Cybersecurity in Germany – Myth and Reality

There is a new threat. We cannot see it, hear it, or feel it, but it is there. It is putting industrialized countries under pressure and targets our infrastructure without any guns being pointed or shots being fired. Its troops are invisible, their attacks silent, and the front has no borders.

The Internet has made our world faster and our economy stronger. It connects people and markets. It links knowledge and ideas. But it opens up a new flank of vulnerability. And it is increasingly a scene of military conflict.

"Net wars" are raging. Meanwhile, experts fight over definitions. When does a military cyberwar begin under international law? When is an Internet attack crime, sabotage or espionage? In the age of cyberwarfare, modern industry is in danger since its digital technology contains numerous weaknesses. Among them, cryptography is a contested field. Experts claim that quantum computers could break virtually any encryption, but critics disagree.

It is undisputed that practically our entire infrastructure is now digitally networked. Now that Internet attacks are a reality, the vulnerability of virtual life has become apparent. Cyberattacks are highly attractive to online criminals. The perpetrators can rarely be identified. They operate internationally, in distributed teams, using fake sender addresses. In a cyberattack, at first no-one really knows who is behind the attack. Is it in fact an enemy power, is it a corporation, is it an organized crime syndicate, or is it an individual hacktivist? It is hard to tell.

In online attacks or cyberwarfare, there is a lack of clarity over what exactly constitutes armed conflict or "war". Opinions on this differ widely. The U.S. State Department regards a cyberattack as an act of war if it causes a particular order of magnitude of damage or death. Possibly, this also implies responses by military means. But so far no-one has managed to determine where exactly the threshold lies.

The German federal government is also grappling with the issue of cyberattacks. As part of its cyber strategy, it is attempting to strengthen preventive measures for IT security in Germany. Cyber interests are an important "cross-cutting issue", it says. Thus, the German Federal Foreign Office has acquired an International Cyber Policy Coordination Staff.

Where do the financial resources come from in Germany, and in an extreme scenario, which states are actually still able to rely on their cyber infrastructure? A build-up of cyber capabilities can be observed. The German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, BSI) is providing IT advice to the German armed forces (*Bundeswehr*). In Tallinn, the NATO and its partners have established the Cooperative Cyber Defence Centre of Excellence against cyberwarfare, while agencies are paying close attention to the security of their own networks. At the same time, all of this provides very strong safeguards for each country's respective own national military infrastructure.

Aside from Internet freedom and defense against cyberattacks, protection against espionage is also becoming an increasingly important theme since most cyberattacks are criminally motivated or originated by foreign intelligence. The protection against those attacks is, therefore, not necessarily a task for the military but rather also for the state. In Germany, the national cyber defence center connects its different agencies. The German federal office for information security (*Bundesamt für Sicherheit in der Informationstechnik*, BSI), the German Federal Intelligence Service (*Bundesnachrichtendienst*, BND), the German Federal Criminal Police Office (*Bundeskriminalamt*, BKA), the German *Bundeswehr* and others are taking care of German security interests and attempting to contain the threat.

Cyberspace is comparable to space, airspace, or the high seas. Even if cyberwarfare threats seem quantitatively unimportant, they have high relevance since they will become part of conventional warfare in the future. Monitoring and correctly interpreting Internet attacks will become an increasingly high priority for any armed forces.

But even today, some incidents which have come to light already demonstrate how delicate an cyberattacks can be, and how unexpectedly they can hit countries all around the world. Malicious software such as *Stuxnet*, which can "log in" by itself when connected via USB, reveals a new form of conflict between states. This is an area which cannot be covered solely by the private sector.

Thereby, cybersecurity is necessarily part of state security precautions, with cyberspace requiring new defense policy as well as military strategies. Especially the military is vulnerable, in particular because modern warfare – whether with tanks, warships or missiles – relies on IT systems. If someone disrupts the electronic systems in a warplane, this can have the same effect as an attack with a conventional anti-aircraft weapon. Furthermore, unfamiliar information and communication systems require specialized IT knowledge.

Dealing with cyber threats therefore requires special resources and well-trained armed forces. According to German defense policy guidelines, the *Bundeswehr* needs to cover this new range of capabilities as well. Like all armed forces, it needs to make its own technical and personnel capacities available to deal with cyberattacks as effectively as with conventional threats. Cyber vulnerability is not a myth. In the foreseeable future, the government will have to give an account of Germany's cyber capabilities.

The digital front is a new global challenge between democracy and freedom, between the NSA and Google, and very different forms of government. This makes it all the more important to discuss resources, possibilities and opinions.

I wish you a pleasant read of our e-journal special.

Gertrud Maria Vaske

Chief Editor

"Ethics and Armed Forces"

Cybersecurity – How Policy Makers Fail

Isabel Skierka *is a research associate with the Global Public Policy Institute in Berlin. Previously, she was a Carlo Schmid fellow at the NATO, and prior to that, she was a trainee with the Task Force for Internet Policy Development at the European Commission. Her work focuses on international security policy, global Internet policy and governance, and European integration. She completed a master's at the War Studies Department of King's College London and holds a bachelor's degree in European studies from Maastricht University with an exchange semester at Sciences Po in Paris.*

Code-based attacks on civilian and military infrastructures pose one of the great new challenges for security policy. Political decision-makers, the security industry and media pundits are increasingly warning of a "cyber-war" that could throw the economy and society into unpredictable turmoil. Despite this rhetoric, such scenarios have yet to materialize.

But the militarization of the digital realm and an ensuing global arms race is already reality. The extension of state-imposed military control over the digital sphere constitutes a threat to freedom, innovation and security of the Internet – with disastrous consequences for human rights and global economic development, and ultimately for national security, which it is supposedly protecting.

In 2012, nearly 50 nations told the United Nations that they were working on military cyber strategies or capabilities. For defense against cyber threats, governments are developing mass electronic surveillance and reconnaissance systems. As an offensive strategy, a number of countries, with the United States, Israel, China and Russia leading the way, are developing capabilities such as weapons based on malicious code. The *Stuxnet* case is a well-known example. The United Kingdom and France, as well as Iran and North Korea, are also striving to acquire offensive cyber capabilities.

Furthermore, the militarization of the digital realm is manifest in how expenditures for military cyber technologies are growing in the midst of shrinking overall defense budgets in the US and Europe. Although the U.S. defense budget for 2015 has decreased in comparison with the previous year, the portion set aside for military "cyber activities" rose to four billion euros, or one percent of defense spending. Last year the U.K. also announced investments in cyber defense and surveillance capabilities totaling one billion euro. China's defense budget rose by more than seven percent this year, and Russia's by around five percent. A large part of these expenditures is likely to be spent on the development of better cyber capabilities.

In light of these developments, it is all the more alarming that there is currently no comprehensive set of norms to regulate cyber-warfare between states. Although the Tallinn Manual, adopted by a number of NATO countries in 2013, formulates some initial rules

for cyberwar, key questions of international law still remain unanswered. For example: At what point does a cyberattack justify a military counterstrike? This is mirrored in the recent extension of the principle of collective defense – as set out in Article 5 of the NATO Washington Treaty - to include cyberattacks. The Alliance does not define the threshold an attack would need to reach in order to trigger the collective defense clause. Therefore, potential attackers and defenders are operating in a gray zone.

The militarization of the digital sphere is directed not only against other states, but increasingly also against the states' own citizens, as demonstrated by the documents Edward Snowden revealed. Authoritarian regimes have long used their national Internet infrastructure for comprehensive censorship and surveillance of their citizens. Here, "information security" is meant to protect the stability of the regime against subversive movements.

While in democracies we are very far away from the Chinese "information security" model, American and European intelligence agencies and militaries do use the Internet for mass surveillance. The National Security Scandal (NSA) scandal has shown how, over many years, decision-makers in the U.S. have collaborated with European intelligence agencies, developing a globally operated military secret service apparatus under the guise of „protecting cybersecurity" and "fighting terrorism." The fact that the director of the NSA is also part of the military speaks volumes.

At the same time, the NSA has also willingly accepted direct weakening of Internet security. Reports show that the agency has compromised at least one international encryption standard issued by the National Institute of Standards and Technology (NIST) in order to gain access to millions of computers. The Snowden documents also show that the NSA gained back-door access to IT products made by American companies, such as routers, servers and other network devices. These purposefully implemented vulnerabilities also provide ways for cybercriminals, hackers and intelligence services of other countries to attack national networks and critical infrastructures that the NSA is tasked to protect. Quite frankly, this is a risky way to handle your own national security. Similar reports emerged a few years ago revealing that the Chinese government had asked its two IT champions *Huawei* and *ZTE* to build back-doors into the program codes of their globally exported products. Such intentional weakening of Internet and product security has devastating consequences for the security of individuals, businesses and governments. It is also a threat to innovation and free trade. The resulting mistrust of foreign IT products and American spy agencies has provoked a new online nationalism in the form of vociferous calls in Europe – and especially in Germany – for national or European solutions to the problem of surveillance and espionage. These include proposals for a European cloud or purely domestic IT production. If such proposals were implemented, the economic damage to the American IT industry and global trade would be substantial.

Instead of falling back on militarization and online nationalism, we need to rethink our security culture. Our prime objective in democratic societies should be to maintain the fundamental pillars of our freedom. The prioritization of military interests must once again give way to a nuanced discussion about what is necessary and feasible. Rethinking cybersecurity policy requires, above all, a clear differentiation between the various forms of threats, and adequate response mechanisms. Although code-based attacks do pose a military threat, cybercrime and cyberespionage are far greater problems. They cost the global economy an estimated US$ 500 billion every

year. But the problem of cybercrime should not be addressed with military measures; it requires effective civilian cooperation, particularly by judicial and police institutions in international law enforcement. Furthermore, in their response to digital threats, decision-makers should involve all relevant civilian stakeholders in politics, business and civil society as well as network operators.

For governments, the greatest challenge lies in helping private network operators, businesses and banks to secure their networks – if necessary, by introducing appropriate legislation. In general, decisions concerning the security of civilian networks should not be left primarily to the military and intelligence agencies. It would be an important step if the governments of Germany and other countries were to do more to encourage investment in secure IT technology in their economic development programs. Here, priority should be given not to the geographical origin of IT products, but to the verifiable security standards these deliver.

In a globalized economy no European or other country is realistically able to source its IT technology exclusively from domestic manufacturers. In large part this technology will have to continue being supplied from overseas. The sole condition should be that, before they are used in the public or private sector, these technologies pass appropriate technical inspection procedures and not include back doors. At the international level, governments should strive for greater cooperation and implement confidence-building measures to prevent any escalation of the digital arms race. A few first steps toward such a process have already been taken at UN level. But due to differing national security interests and understandings of security, it is very unlikely that governments will sign an international cybersecurity treaty in the near future. Instead, international cooperation could take place within less formal mechanisms, based on common and less politically charged interests. All countries share an interest in the reliable functioning of the Internet and in controlling cybercrime. For example, signatories to the 2001 Convention on Cybercrime of the Council of Europe include not only the member states of the Council of Europe but also non-European countries such as the United States, Japan and South Korea, thus extending its reach to other parts of the world. Governments could also work to enhance existing cooperation between technological institutions such as Computer Emergency Response Teams (CERTs) and other stakeholders, e.g. network operators and Internet providers. These informal efforts for Internet security could help to create international security standards as a basis for cooperation in other areas. Every individual user would benefit from such a strengthening of security on the Web. At the national level, democratic governments should strive to ensure that parliaments have better control over their intelligence services and militaries. This is precisely what distinguishes them from authoritarian regimes. Unfortunately, the NSA, like the Government Communications Headquarters (GCHQ) in the U.K., is subject to insufficient oversight by the legislative and judiciary. In Germany, too, judicial and parliamentary control over the German Federal Intelligence Service (*Bundesnachrichtendienst*, BND) is deficient.

Freedom of the individual must remain at the heart of security policy in the digital age – that would be the strongest pillar guaranteeing both national and international security.

Interview with Felix *FX* Lindner, Hacker

Felix *FX* Lindner *hacked BlackBerry, the network of Cisco, and the energy supply of a German town. He is a well-known expert in the computer security community. Over the last decade he has presented his research at conferences around the world and made it freely available on the Internet. He is the founder as well as technical and research head of Recurity Labs GmbH, a high-end security consulting and research team that specializes in code analysis and the design of secure systems and protocols.*

What do you think is the biggest threat from cyberwarfare? What do you think was the biggest threat to data security and data protection in 2014?

I think the biggest threats arise from a lack of understanding among many of the people who are in positions of responsibility. As a result, just a few people determined the media narrative and political agenda in 2013 and 2014. Unfortunately, objective discussions about data security strategies are as rare as they are urgently needed.

What are the dangers of cyberwarfare, primarily for the military, but also for the civilian population and for businesses?

The main issue in all three areas is a blinkered obsession with computerization. We can't safeguard our existing computer systems and networks, yet everywhere we keep on integrating an ever greater number of more deeply networked computers – whether in weapons systems or supply infrastructure for electricity, water and gas. In many cases the benefit is illusory at best, whereas the added dangers are very real.

Cyberattacks could disable weapons systems such as anti-aircraft missiles. Why isn't this done more often?

For one thing, the necessary knowledge and personnel with the corresponding skills are thin on the ground. As long as conventional means are available to achieve the same effect, it is not worth using this scare resource. Also, because of their lack of specialist knowledge, the decision-makers in the military and government have a justified fear of secondary effects, which they are unable to assess.

Could cyberattacks be a way of containing current conflicts (Syria/Ukraine)?

Cyberattacks are not suited to this purpose. Offensive means are generally not the right way to defuse conflicts.

Supposing I was Defense Secretary, should I spend money on cyber weapons or cybersecurity, or would it be better to spend money on conventional weapons?

The decision should be the result of an overall security policy strategy, which a Defense Secretary hopefully has.

Developing offensive capabilities *on a par* with those of other countries is certainly essential, since the fifth domain is not going to simply disappear again. And just as you can't order an air force on *Amazon* and have it show up the next day, cyber offensive forces require

many years of training before they are ready for deployment.

Cybersecurity, as it is called, requires more of an integrated policy approach.

What does it take to disable a country's infrastructure?

In terms of a cyberattack – all it takes is a few capable attackers with a lack of scruples and enough money to pay for them. But if you're not in any rush, extensive privatization is also a very effective method.

The cyber weapons *Stuxnet* and *Flame* created a stir. They were used to spy on and attack the Iranian nuclear weapons program. What was particularly dangerous about that?

The collateral damage was particularly dangerous, and not the immediately obvious damage. Take *Flame*, for example. A cryptographic signature was generated so that it looked as if the file came from *Microsoft*. This circumvented many security checks that are essential for a whole series of protection measures in computer security. The method still works today, but it's not easy to just replace the protection measures. As a result, the whole world is more vulnerable than it was before.

Demystification of cyberwarfare – it is often said that no such thing exists and that it is not new. At our Berlin panel discussion, in response to the claim that malicious software wears no uniform, you said that military attacks in the Internet wore more of a uniform than Russian soldiers in the Crimea. What did you mean by that?

Nearly all states place little hope in the medium-term availability of defensive measures, and are therefore focusing on offensive means. Accordingly, the aim is to show everyone else what they can do, as a kind of show of force. The hope is to achieve a certain level of deterrence. But for that to work, it has to be obvious who planned and carried out the attack. So not much is concealed.

How much cyber power does China or Russia have in comparison with the United States?

China and Russia have about the same offensive strength as the United States, although each in somewhat different form.

Who are the current cyber superpowers?

Google, China, Russia and the United States.

So countries that produce computers themselves have a good chance of being or becoming a cyber superpower. What are the chances for Germany at the moment? After Zuse, do we still matter in the world of computer technology?

No, Germany doesn't play an important role any more. It's a shame especially because the skills are available, but they aren't used.

How do cyber attackers operate? How do they go about attacking a country, corporations, businesses, the government, or the intelligence services?

They're a bit like burglars: they collect background information, scout out the target, try the doors and windows, choose their tools, then break in. Unlike burglars, instead of making their getaway, they barricade themselves inside the building as inconspicuously as possible.

What defense mechanisms exist to guard against intruders? Shouldn't we build our own computers?

Yes, we really should build our own computers. If, unlike everyone else, we also accepted product liability for these computers, while they would be significantly more expensive, they would also be a massive export hit.

Is there a sure-fire way to prevent cyberattackers, such as reverting to typewriters?

If you want to keep a secret, you shouldn't put it on a computer nowadays.

Let's look to the year ahead. Nation states increasingly attacking each other with malicious software. The respective private sectors are affected and activists too will continue to use the Internet for their own purposes. What is the absolute worst-case scenario for Germany? And what scenario could rapidly become reality?

Unfortunately there are many. But I believe that you shouldn't make any instructions publicly available.

How can you prevent any of those scenarios?

An overall policy debate would be a good start.

Is it possible to disable an airport using a simple computer? Can you give us a rough estimate of how many people you think would know how to do that?

Definitely a few thousand people around the world.

Some voices are getting louder: scaremongering and demanding information. What do you think manufacturers of software and hardware products should be doing to improve computer security?

It would be nice if the manufacturers would finally be honest with politicians. Endless new promises about the next miracle product don't get us anywhere. Admitting that the absence of liability on their part is the core problem would make a massive difference. Policymakers won't just go and demand that they accept this liability, since no-one wants to ruin *SAP* & co. But unfortunately the current charlatanry is too lucrative to give up voluntarily.

According to Thomas Ried, cyberwar is just a clever strategy by security firms, since in his opinion it doesn't really exist. What do you think about Ried's theory?

Using a term like "cyberwar" is an excellent way to promote sales of the next miracle product. But that doesn't explain the hundreds of soldiers and hordes of specialists in the defense industries in various countries who are engaged with the issue of offensive capacities, nor the large sums in the corresponding budgets. Ried describes a symptom, not the disease.

What is your assessment of the general security situation for German businesses?

I think that German businesses are extremely exposed. We are an export country that specializes in process and production knowledge. So, unlike raw materials, our export goods are perfectly suited to being stolen (i.e. copied) from our computers, without us noticing.

Analysts calculate that targeted hacker attacks cause millions of euros of damage each year. Do you think that the majority of CIOs and IT managers are currently able to implement correct and useful protective measures?

No, partly because CEOs make it the IT manager's responsibility, as if the CEO had nothing to do with it.

Will security be sacrificed for convenience in the future? With Internet access in German army barracks, how safe from hackers is an e-mail address in the German army?

Security is always being sacrificed for the sake of convenience or vanity. Businesses made major efforts over many years to create a halfway reliable infrastructure with *BlackBerry* – and then CEOs wanted *iPhones* instead.

The security of an e-mail within the German army is something can easily be tested. Unfortunately that hardly ever happens, because

no-one wants to hear the answer they're afraid of.

Experts claim that not a single cyberattack has taken place to date. And yet cyberwarfare is discussed time and again. Is this a strategy by security firms, marketing experts and media analysts, and is cyberwar actually not real?

Whether cyberattacks have taken place is a question of definitions, which is why it is disputed. But we are definitely seeing a continuous increase in activities by nation states. Sorry to say that's not marketing, however much I wish it was.

What makes a good professional hacker?

Integrity, passion, specialist knowledge and skills, and knowing when to stop.

Should hackers fear for their lives, and how timid are the intelligence services?

It is something of a rarity to hear about violent deaths with a possible connection to the intelligence services. More frequently, hackers who have worked for criminal organizations are found dead once the job is done.

Below the threshold of an armed conflict, what kinds of regulation are needed?

As mentioned earlier, I think the greatest need is to introduce product liability for hardware and software, at least when the products are supplied to the state or to the military. As long as it's more profitable to sell completely defective merchandise, so that you can then sell the next version as well, there is no money to be made in secure computers, so no-one makes them.

A question about the extent and threat of surveillance. What would you say to a head of government who uses the *Google* e-mail service *Gmail*, surfs the Web with the *Google* browser *Chrome*, and uses a smartphone with the *Google* operating system *Android*?

I would ask why he or she wastes taxpayers' money on ministries for defense, espionage and counter-espionage, since this behavior makes a mockery of them. I would also be interested to know how far their oath of office is compatible with a complete, negligent surrender of the state to a transnational superpower.

NATO experts published the Tallinn Manual in 2013, a guide that examines how international law should be applied to cyberwarfare, for example. Does this manual have any significance for hackers?

No, those are policy issues.

***Google*/*Apple*/*Microsoft* – to what extent are these companies a danger to personal and national security?**

Google's control over the entire Internet should occupy a prominent position in questions of national security.

What international cyber protection laws do we need?

We should establish international rules that leave control over the Internet in the hands of democratic countries, even though they are a minority of all countries in the world.

And what product security legislation such as product liability do we need to ensure the security of computers and software?

Full product delivery (not a license) and corresponding product liability for software acquired by the German federal government and army is the first and most important step. After chaotic beginnings, you will see a dramatic rise in quality, security included.

As a purely hypothetical question, in the event of a cyberattack, would you hack for Germany in a camouflage suit?

I help various countries to better defend their infrastructure. So far I've never needed a camouflage suit to do that.

Questions by Gertrud Maria Vaske, chief editor of "Ethics and Armed Forces"

Interview with Michael Hange, president of BSI Germany

Michael Hange *is the president of the German Federal Office for Information Security (BSI). Since the foundation of the German National Cyber Defense Center under BSI's jurisdiction, he has been its spokesperson. From 1994 until early 2009 he was vice-president of the BSI, and until October 2009 was a permanent representative of the IT director in the German Federal Ministry of the Interior. He has a degree in mathematics and has worked in IT security within the German federal administration since 1977.*

At the beginning of 2011, people still laughed at the idea. "In Germany there is incessantly some form of attack on the Internet." But the German federal government was being serious, and the cabinet approved a cybersecurity strategy for Germany. Three years later, what has become of the cybersecurity strategy?

Cyberattacks take place on a daily basis. They affect not only businesses but also government and private users. Attacks are becoming more professional and more targeted. Back in 1991, the growing importance of information security was institutionally acknowledged with the formation of the German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, BSI). Of course, the situation has changed dramatically since 1991 as a result of greater IT penetration and interconnectedness – which has brought a sharp rise in the number of attractive attack targets – while attackers exploit the anonymity of the Internet. The German federal government's 2011 cybersecurity strategy is still in force, and at the moment, for example, we are continuing to develop our National Cyber Defense Center (*Nationales Cyber-Abwehrzentrum*, NCAZ), which is geared to prevention.

How great is the threat to our country's security?

Cyberattacks happen every day, and affect all target groups, the government and administration just as much as businesses and private users. Attacks are becoming more professional and more targeted. A threat to citizens, for example, is identity theft, which is becoming a daily phenomenon. As far as businesses are concerned, there is always a threat wherever you have anything of value. Especially in Germany, very many small and medium-sized enterprises are considered to be particularly innovative. They possess extensive specialized knowledge and expertise, many are "hidden champions", and lots of firms own patents and important intellectual property. That inspires covetousness. So it's a mistake for businesses to think that being small makes them safe, or to assume that not being widely known means they are at low risk of cyberattacks. Patents and research findings from a small business can be just as lucrative for attackers as the management board decisions of a major corporation.

In the case of businesses, Internet-based attacks can have a considerable impact on our economic prosperity and technological competitiveness. What are you doing to prevent this?

Businesses are essentially responsible for protecting themselves against cyberattacks. But when it comes to critical infrastructures and maintaining business processes and services that are clearly in the common interest in Germany, then the state should intervene in a protective capacity. This is why the German Federal Ministry of the Interior has produced a draft bill for an IT Security Act that addresses these aspects.

The German Federal Court of Auditors (Bundesrechnungshof) had doubts about the effectiveness of the National Cyber Defense Center, saying it was unsuited to pooling defense capabilities against online attacks, and that there was just a single daily briefing. Specifically, they said that the Defense Center was "not suitable for pooling the competences and capabilities distributed across government institutions for defense against attacks from cyberspace". What do you think about that?

Since the Federal Court of Auditors has not yet completed its review of the Cyber Defense Center, I do not wish to say anything more on the subject.

What kind of security do you offer for users?

As a national security authority, the Federal Office for Information Security (BSI) has the goal of promoting IT security in Germany. We are primarily the central IT security provider for the German federal government. But as part of what we do, we also turn to manufacturers as well as private and commercial users and providers of information technology, since only concerted action can be effective.

Cybersecurity strategy – malicious software is installed unnoticed in businesses, in homes. What can you do if legitimate websites are suddenly manipulated – a case for the German Federal Criminal Police Office (*Bundeskriminalamt*, BKA) – and how do you do it?

The respective operators are responsible for the security of websites. If BSI receives information concerning websites that are distributing malware, BSI will usually inform the operators, who should then take steps to disinfect the site.

To what extent do you assist the German armed forces (*Bundeswehr*) in cyber defense?

BSI is a civilian and preventive authority. More particularly, it has a protective function for key government networks. BSI detects targeted and non-targeted attacks on key government networks and defends against these attacks, in its role as an IT security provider. BSI's further responsibilities include approval of IT security products and services used within the German federal government. This leads to cooperation between the German Federal Ministry of Defense and BSI. The *Bundeswehr* is responsible for cyber defense in the military sense.

The threat from botnets, which generally comprise infected PCs owned by private users, has also increased. Botnets are now being professionally leased and used for IT attacks. The motive is often financial gain. To this can be added "hacktivism", as a means of expressing political views via IT attacks, for example. In view of the rapid spread of smartphones, tablets and netbooks, attacks and eavesdropping using mobile devices are an increasing danger. Even members of the German Parliament (*Bundestag*) are coming to you. What remedies are effective against this threat?

Here you need to distinguish between the individual phenomena. Botnets are indeed a threat to IT security in Germany. To prevent

their computer becoming part of a botnet, users should follow the security advice issued by BSI, which we provide e.g. on our website www.bsi-fuer-buerger.de. As far as mobile communication is concerned, here too there are new challenges. More and more people are using and benefiting from smartphones. But you should keep an eye on the risks and modify your behavior accordingly, e.g. with regard to installing apps or using interfaces such as Bluetooth and WLAN.

Your website www.bsi-fuer-buerger.de and the warning service www.buerger-cert.de provide current information and recommendations for businesses. In addition, BSI supports initiatives by civil society groups to enhance IT security for the public and for businesses. Electronic identities and De-Mail are further approaches that BSI is taking to increase the level of IT security. How many visits do you get each day?

The BSI cybersecurity recommendations are aimed at businesses and professional users, not at the general public. The recommendations that we publish within the Alliance for Cyber Security have been very well accepted. The alliance recently welcomed its 1,000th member. In the space of just two years, the Alliance for Cyber Security has become an established platform for discussing cybersecurity issues.

How can businesses protect themselves against economic and industrial espionage? What is the most important thing they should do?

Awareness of IT security issues has increased – we have noticed this in many talks with business representatives. That is an important first step. There is still some work to be done in terms of implementing security measures, including some standard measures. IT security is a diverse field that includes organizational and human resource aspects as well as technological measures. The procedures set out in the BSI "Basic Protection Catalogues" have become established as a standard concept for information security. The IT-*Grundschutz* (or "basic protection for IT") scheme helps in the development of a security organization and also provides a comprehensive basis for risk assessment, reviewing the existing security level and implementing appropriate information security. We advise smaller businesses to stay informed about IT security, e.g. via the Alliance for Cyber Security website. The alliance offers an extensive and constantly growing knowledge base plus the opportunity for confidential dialog with other members, as a way to benefit from each other's experiences.

Experts such as Dr. Sandro Gaycken claim that it is impossible for computers and software as we know them to be secure. Do you agree?

It is true that it is not possible to achieve one-hundred-percent security. Software is usually made by people, and people make mistakes. But not every error is automatically a security problem. Systematic implementation of standard security measures provides protection against more than 80 percent of known cyberattacks.

How many attacks currently take place every day or year?

The German government network is subject to thousands of non-targeted attacks every day. These are primarily broad-based attacks. But every day we also see three to five targeted attacks on the government network.

What does the Snowden affair mean for the digital arms build-up?

It was known that foreign intelligence services posed a threat in principle, but the extent of their activities was not known. It is important and right to be addressing this issue, but it not should direct attention away from other threat scenarios such as cybercrime.

What do you think about the idea of creating more or less reliable European systems that meet strict data-privacy and rights-protection criteria?

The Internet is and remains global, and offers enormous capabilities for private as well as business users. We should preserve these capabilities, but we must not ignore the risks.

At the moment, Internet infrastructure is clearly dominated by non-European products. It is not realistic to challenge this dominance in the short term. It is more expedient to ask non-European providers to ensure greater transparency. Also, it should be possible to protect non-European system components like routers with national, trusted crypto-algorithms, and so achieve sovereignty over our own communication.

Questions by Gertrud Maria Vaske, chief editor of "Ethics and Armed Forces"

Imprint

The e-journal "Ethics and Armed Forces" (ISSN 2199-4137) is a free-of-charge, non-commercial, digital publication containing journalistic and editorial content.

It is produced by

Zentrum für ethische Bildung in den Streitkräften – zebis
Herrengraben 4
20459 Hamburg
Germany

Director of zebis: Dr. Veronika Bock

Contact zebis

Phone: +49 (0)40 67 08 59-51

Fax: +49 (0)40 67 08 59-30

E-mail: info@zebis.eu

Person responsible for content pursuant to section 55 (2) of the German Interstate Broadcasting Agreement (Rundfunkstaatsvertrag, RStV):

Gertrud Maria Vaske
Herrengraben 4
20459 Hamburg
Germany

Service provider as the legal entity of Zentrum für ethische Bildung in den Streitkräften – zebis:

Katholische Soldatenseelsorge (KS)

Legal form

Public-law institution

Supervision

Catholic military bishop for the German armed forces (Bundeswehr)
Am Weidendamm 2
10117 Berlin
Germany

Authorized board of directors of KS:

Leitender Militärdekan Msgr. Wolfgang Schilk
Am Weidendamm 2
10117 Berlin, Germany

Diplom-Kaufmann Wolfgang Wurmb
Am Weidendamm 2
10117 Berlin, Germany

Contact KS

Phone: +49 (0)30 20617-500

Fax: +49 (0)30 20617-599

E-Mail: Info@Katholische-Soldatenseelsorge.de