S+F Sicherheit und Frieden
Security and Peace
1 2014
32. Jahrgang
S. 1–79

THEMENSCHWERPUNKT

Roots Unknown – Cyberconflict Past, Present & Future

Alexander Klimburg*

Abstract: The rise of cyberspace as a domain of activity is one of the most significant developments in the history of conflict. The increased focus on "information" as a weapon itself, rather than being simply a facilitator of weapons, is changing also how both conflict and political power are perceived. While the most important facet of power used to be the ability to coerce one's opponent by the use of force, now the ability to set one's opponent's agenda and even preferences is becoming a realistic alternative. Also, it provides governments with new ways of projecting power internally (within their borders) as well as internationally, changing the meaning of "international security". This means that the future development of cyberspace and cyber conflict is very much tied to the development of "Internet governance" – the practice of managing the world's Internet resources.

Keywords: Cyberspace, cyber conflict, cyber warfare, cyber security, web attacks
Cyberraum, Cyberkonflikt, Cyberkrieg, Internetsicherheit, Internetattacken

If there is something everyone can agree on, it's that the rise of cyberspace as a domain of human interaction represents a development of historic proportions. The changes of the last decade – let alone two decades – are truly staggering. In 1993 the TIME Magazine ran a title page on the new culture of "cyberpunks", and in the same year RAND published a benchmark study with the scary title: "Cyber war is coming!" Despite this, in 1993 only extremely few people had even heard of the Internet. In 1993 the Internet probably had less than 1 million users, which exploded to 16 million by 1995.[1] By 2013 that number has risen to over 2.75 *billion* users – or around 39% of the worldwide population. As we increasingly move towards the aptly-named "Internet of Things", human actions in cyberspace will be vastly outnumbered by those of their gadgets – each of which could easily have many Internet protocol numbers assigned to subcomponents, from a toaster coil to a clothing lapel to a car battery. The need for new Internet identifiers is so great that the original identifier list (which,

* Alexander Klimburg is Senior Adviser at the Austrian Institute for International Affairs and Fellow of the Harvard Kennedy School. Since 2006, Mr. Klimburg has acted as an adviser to a number of different governments and international organizations on various issues within cyber security, Critical Infrastructure Protection (CIP), and EU Common and Foreign Security Policy (CFSP).
The following article will also appear as Nato Defence College Research Paper.

1 Internet World Statistics, „Internet Growth Statistics", 2013 http://www.internetworldstats.com/emarketing.htm.

among other things, is the long string of digits that lurk behind a web address) actually ran out in early 2011 – and that accounted for 4.3 billion unique identifiers. The new shift to version six (from version four) of the Internet Protocol will provide for a little more room – 340 billion unique identifiers – which means that we should not run out of space anytime soon – depending on what the future of the Internet holds.

But what will the future of the Internet look like, and, by extension, what will the future of conflict in cyberspace be? These very simple sounding questions are in fact enormously difficult to answer, as among experts there is little agreement on the key variables. A significant problem is that "power" in cyberspace is by no means a clear-cut subject, and the different understandings here derive from different views on exactly how significant a development the rise of cyberspace truly is. Our individual views on the development of the Internet and cyberspace are very much contingent on how big a development we think it is within the overall history of human conflict. Some countries view the rise of cyberspace as easily encapsulated within existing doctrines and international norms, while other countries, which have long emphasized the importance of "information control" in their own doctrines, have a more transformative view. It is these countries who also see their interests most at threat from the rise of cyberspace, and who are most likely to try to dominate the international agenda in the future.

1. How Big a Revolution? Different Views on the Advent of Cyber Conflict

There are widely diverging views as to how significant the advent of cyberspace is within the wider historical context, and, in particular, how important it is within the history of human conflict. In essence, there are three different versions of how big a development "cyber" really is – and they differ greatly from each other. In fact, the difference is so significant that, as we will see, they are in effect irreconcilable with each other – and therefore vary dramatically as to their view on how much cyberspace can be considered a mere incremental modification, a gradual development or a radical paradigm shift of the prevailing conflict paradigm.

The "incrementalists" are those who are least impressed with the rise of cyberspace. Even if they themselves do describe it (and their own thinking) as revolutionary, their own historic comparisons show how limited that revolution really is perceived to be. In broader terms, they see the rise of cyberspace as the beginning of the "third wave of industrialization"[2][3] – in many ways simply the continuation of a trend first initiated by the mass introduction of the spinning jenny. Both the concept of "Revolution in Military Affairs" (RMA) as well as the doctrine of "Network Centric Warfare" (NCW) clearly falls into this category. According to this view, cyberspace only adds certain subsidiary elements to human conflict and the waging of war – usually just supporting the actual physical destruction of an enemy by increasing the "self-synchronization" and situational-awareness of the war fighters. Thus, "cyber" mostly functions as an adjunct to present war fighting capabilities (i.e. electronic warfare or psychological operations), and does not have a truly transformative character – beyond the superior effects of synchronization of combat power through greatly enhanced tactical and operational communication.[4] The value of NCW was first shown in the 1991Gulf War, and clearly came into its own in Operation Iraqi Freedom, where it helped to achieve stunning successes on the battlefield. Likewise, however, those successes were not easily translated into a lasting victory off the battlefield, where NCW proved less helpful in understanding the new dimension of conflict.

Following the "incrementalists" comes what could be referred to as the "gradualist" faction. The gradualists consider themselves the true revolutionaries within military thought, although some would say that what is most striking is the "essential banality" of their concepts.[5] In particular, this includes the "Generation Warfare" (GW)[6] adherents, who since the late 1980s have tried to put technological developments in warfare within a wider historical context. This effort is generally considered laudable but equally fraught with contradictions. From the point of view of cyber security, the emphasis of considering "cyber war" as an example of Fourth-Generation Warfare (4GW) – or even 5GW – is in many ways positive for its emphasis on a "lack of center of gravity", or for its consideration of the importance of non-state actors. However, it also proves insufficient in that it seems to consider that conflict really is about imposing ones will over a resisting enemy – rather than forming the conditions under which they might perceive victory to be possible at all. The historical analogies of the GW concept are also somewhat suspect: did warfare really only start with Napoleon and gunpowder, and are these "generations" really as mutually exclusive as they seem to apply? Detractors like to point out that even an ancient general such as Alexander the Great had to deal with insurgents and "4GW".

The "radicals", by contrast, do not think that the linear development of the history of warfare only starts with the Napoleonic armies. They do not think that the advent of cyber conflict is simply an adjunct or modification of gunpowder-defined conflict. At the very least, "radicals" would consider cyber conflict itself to be as big a paradigm shift as the (equally prolonged) introduction of gunpowder. Some might even go further and say that the only historical analogies that can be drawn are those that relate to the appropriation of new domains of conflict (i.e. sea, land, air and space) rather than to the introduction of specific technologies. Only one of these domains – air – was actually "conquered" exclusively under the use of a single specific technology – namely gunpowder. The

2 Jeremy Rifkin, The Third Industrial Revolution. How Lateral Power Is Transforming Energy, the Economy, and the World, Palgrave Macmillan, 2013.

3 Robert J. Gordon, „Why Innovation Won't Save Us", The Wall Street Journal, 21 December 2012.

4 Interestingly, the Effect-Based Operations (EBO) concept, which has largely fallen out of favor, showed elements of understanding the multifaceted nature of cyber better than NCW.

5 Anthony D. McIvor (Ed.), Rethinking the Principles of War, Naval Institute Press, 2005.

6 The „Generation Warfare" (GW) concept starts with Napoleon and „mass warfare" (1GW), proceeds to firepower and WWI (2GW), maneuver and WW II (3GW), and leads to the present-day emphasis on networks and insurgency warfare (4GW).

others, including land and sea (let us consider space as of yet unconquered) are domains that are constantly expanding and retracting in their importance, and where different technologies have played different roles. Within these domains the struggle for dominance is therefore constant and partially a function of technological change. Correspondingly, cyberspace is not a "technology" itself but a domain within which many different technologies may be applied and, more importantly, which can be used to project ones will on the adversary. Most importantly, this can be done without the adversary actually knowing that this is occurring. "Radicals" would say it is possible to be at war without actually realizing you are at war.

2. The Three Faces of (Cyber) Power?

Put differently, each of the three fundamental views of cyber conflict map very well to what political science has long considered the "three faces of power".[7] These "faces" of power are valued differently in different countries, and understanding these different preferences is absolutely vital in helping to understanding national priorities.

The first face of power is the most obvious – within a "hard power" context it is the traditional "coercing" of the enemy through the application (or threat of application) of force. This is the standard "bend to your will"-approach that most military philosophies by their very nature are concentrated on. The second face of power is more subtle – it is the "agenda setting" that allows actors to frame the context under which victory or defeat can be measured. In diplomatic context this could include arms control treaties or similar binding agreements. Finally, the third-face is "preference shaping" – the most subtle variant of power. Here the adversary not only obeys the agenda that was externally set, but even their very preferences within that agenda are pre-determined, maybe even unknown to them.

For those who think that this type of thinking is without any practical grounding, consider the Soviet military theoretical development of "Reflexive Control" (RC), a perfect example of a strategic "third face of power"-doctrine. RC had a very clear mission statement, namely as "a means of conveying to a partner or an opponent specially prepared information to incline him to *voluntarily* (emphasis added) make the predetermined decision".[8] In essence, in RC thought, a war can be declared, fought and even won without the enemy ever knowing that such a state of conflict even existed. One example of what some Russians to this day consider an example of RC thought was the US "Strategic Defence Initiative" (SDI) of the 1980s. The Soviet Union was effectively "tricked" into wasting billions of ill-afforded Rubles to keep up with the so-called "star wars program", money it desperately needed elsewhere.[9] Some observers consider RC thought to be essential to Russian, and also Chinese, approaches to "cyber warfare."[10]

Why is this important? Because these three views of the importance of cyberspace for conflict are closely connected to how different governments perceive cyber conflict overall, and how they want the issue to be dealt with on the international stage. The interesting contradiction is that those countries that are widely agreed to have benefited the most from the rise of cyberspace are those who seem to have the least "revolutionary" view of its importance – a view that is prevalent in China and Russia, to name but two examples.

The United States – which was at least a decade ahead of all others in the application of "cyber" elements to national security – seems to adhere to a relatively conservative view of its application, as witnessed to the role that Computer Network Operations (CNO) has within Information Operations (IO)[11] – itself a more operational rather than strategic concept. Likewise, the United States has long argued that no aspect of state conflict needs to be treated differently in cyberspace than in traditional International Law. The US, as most Western nations, have pushed for the applicability of the International Humanitarian Law and the related conventions – for instance the Geneva or Hague conventions – to cyber conflict.

Russia and China, in contrast, have a more "radical" view of cyber – viewing it as something potentially completely new and, from their point of view, exceedingly dangerous. These countries have clearly stated that they view "information" as potentially the most destructive of weapons, as made very clear in documents such as the Russian Information Security Doctrine or the Chinese "Three Warfare's" concept – "psychological information attack" can be as harmful, or even more harmful, than "technological information attack". In their view, "the national information sphere" (a favorite word of Russian diplomats) is vital strategic terrain that is absolutely essential to the national welfare – which often of course can be construed as including the category "regime/government stability" – and one, which must be defended from foreign interference, let alone control or domination. To lose control over this "national information sphere" is in many ways worse than to face defeat on a foreign battlefield.

What exactly constitutes such an interference – or indeed threat of domination – of a "national cyberspace" is not only a question that concerns countries such as Russia and China, and forms the essence of what can be considered the *"first face"* of power in cyberspace – the ability to directly and physically control the flow of information, for instance in order to facilitate a cyber-attack. In particular, this can include the threat of contaminated or suspect hardware being resident within one's core networks, or the subverting of critical Internet services from the inside. So-called "Hardware-based attacks" are very hard to protect against as they occur effectively behind the firewalls and can hide their attacks as being legitimate behavior. The United States, for instance, has repeatedly blocked the

7 For a discussion on this, see Joseph S. Nye, The Future of Power, Public Affairs, 2011.

8 For a fascinating application of RC theory in the modern environment, see National Research Council, Disrupting Improvised Explosive Device. Terror Campaigns. Basic Research Opportunities. A Research Report, The National Academies Press, 2008.

9 See for instance Tim Thomas at http://fmso.leavenworth.army.mil/documents/psyop/psyop.htm.

10 For an excellent summary of RC and an analysis of its relevance for cyber, see Franklin D. Kramer et al. (Eds.), Cyberpower and National Security, National Defense University Press and Potomac Books, Inc., 2009.

11 As defined in JP 3-13, which, although it has been superseded by other recent documents, still clearly shows the context of CNO.

entry of Chinese hardware manufactures on national security grounds, and even maintains a "trusted foundry" program to ascertain that certain microchips intended for the most secure systems are "guaranteed" to be safe. Likewise, Russian and Chinese companies have discriminated against US companies for the same reasons. Not only hardware or software companies can be considered sensitive – the same applies to companies that perform specific Internet-related functions, such as the national registries (that manage the national domains such as .de or .uk; for instance the company responsible for the .uk domain is Nominet) or indeed companies that are responsible for specific services, such as security certificates. An attack on the Dutch company Diginotar in 2011, a major provider of Internet security certificates (used to validate secure Internet connections and prove identities) provoked the first official cyber crisis in the Netherlands, and the rapid de facto nationalization of the company.

A *second face* is more difficult for most Western governments to openly acknowledge, and that is that of the overall power of norms and standards. As explained by Joseph Nye, this "second face of power" allows the conditions of international behavior to be set, by creating international norms that limit the choices that actors have. Norms can be rather obvious – such as the operational International Organization for Standardization (ISO) norms that exist for a wide variety of technical tasks such as for civil engineers, electrical technicians, or indeed even medical professionals.[12] However, "Human Rights" can also be considered a "norm" and is often actively interpreted by more authoritarian regimes as being exactly that – simply another tool of *Realpolitik* forced upon by Western powers, to be used as a cudgel when it is in their interest, and to be ignored when it does not. While it is probably true that the OECD nations benefit more from international norm making then other countries do, the West does not always "win" at this game – especially when the West is outvoted in an international context. Such a situation may have occurred within the context of a large ITU[13] conference in Dubai in December 2012, where a cherished Western norm on Internet governance was openly challenged by a majority of the world's nations – more on this later.

The *third face* is the most difficult one for liberal democracies to accept – and that is evident, direct and overt attempts to control the entirety of information consumed by a national population and therefore to help form individual personal agendas. Previously, this category would simply be explained with propaganda and censorship, and overall the Internet does provide much more subtle and invasive methods to accomplish what in effect is the same thing. The legions of Chinese censors that man the great firewall and constantly scan the Chinese Internet for suspect blog posts are only one incarnation of this trend. In Russia, direct and obvious online censorship is much less obvious, although it does occur – Russian legislation and practice has given the security services much more insight into its "national" Internet than perhaps any other country, and uncomfortable information and posts are known to disappear relatively quickly from Russian cyberspace. The Russian viewpoint on this is fairly transparent and has been clear since at least over a decade – the Russian government clearly stated in the "Information Security Doctrine" of 2000 that "maintaining public harmony and [of] the spiritual renewal of Russia" is a major concern. This has its logical conclusion in the new restrictions imposed on the operations of (Russian) NGOs that are recipient of any foreign financing – in which case, since 2012, they have been obliged to register themselves as "foreign agents". Away from the media bluster, the underlying notion is that the foreign interests are actively trying to form opinions among the Russian population – incorrect only as much as these "foreign interests" are seemingly always an equivalent to "foreign governments", as the Russian government seems to consistently have a conceptual problem with the idea of an independent civil society. It needs to be pointed out that this distrust of "foreign NGOs" and the inability to tolerate, let alone trust in international civil society bodies is far from being only a Russian problem.

Overall, the "third face of cyber power" is often cast as being an issue of cybercrime – more precisely, "illegal content". As a matter of international law enforcement cooperation, countries such as China could insist on international support to take down media that would violate its laws – such as (to use but one example) Falun Gong websites or similar content. Of course, China can already block access to such websites – and indeed puts much effort into this activity – but, as Western counter-cybercrime experience has shown, simply blocking websites is most often not effective. A much more effective tool is the internationally used "Notice and Take Down" (NTD) practice to force the hosts of illegal content to take down and possibly even confiscate the content directly. This has been highly effective for combating many types of illegal content – including torrent-index websites (for file sharing), pornography, and, in countries like Austria and Germany, neo-Nazi propaganda. China, as well as many other countries, is presumed to want to apply a much wider NTD regime, one that would effectively force the international prosecution of providers of all kinds of "illegal content", especially of course of a political nature. This would either be a monstrous enforcement of a global censorship regime, from one point of view, or simply the extension of modern law enforcement cooperation, from another.

For obvious reasons, this issue is so heavily charged that most liberal democracies refuse to have any other discussions on international cybercrime cooperation beyond that which was already agreed in the Council of Europe Convention on Cybercrime – to date the only international agreement in force. Even attempts to "bridge" the debate by agreeing to only combat what a Chinese delegation once referred to as "doubly illegal" content (e.g. child pornography or similar) and, "for the moment" not to talk about other types of illegal activity, have been met with resistance. The fear is that such an agreement would be a slippery slope entrapping Western democracies in the international obligation to suppress freedom of speech.

Indeed, "freedom of speech" and the associated concept of human rights (itself a global norm and therefore arguable a "second face of cyber power") has been the standard Western counter to these efforts for a number of years. Many Western

12 Including for operational cyber security – information assurance (ISO 27000 series).

13 The International Telecommunications Union (ITU) is a UN agency responsible for negotiating international norms and standards in telecommunications.

democracies have sought to intimately connect the human rights and Internet usage, and have interpreted the most applicable human rights convention (the International Covenant on Civil and Political Rights, ICCPR) to apply, together with all its exceptions regarding national security and similar aspects. Despite the exceptions that human rights conventions make for national security issues, there are obvious holes in the Western democracies' positions – see any type of "illegal content" on political grounds – and these are used as examples of inconsistency and hypocrisy when arguing to undecided third nations, in particular in South America and Africa.

The "three faces of political power"[14] is a social sciences concept that can certainly be applied to international cyber security. Overall, it can be said that each "face" of political power becomes correspondingly more difficult to purposely influence or, from the point of view of any single entity, control. The "third face of power" is very difficult indeed to purposely project. Of course, power can also be projected unconsciously – a government, just like a country, culture, or even sub-culture can have this influence without actively seeking it. But the effect on the recipient is the same.

The great difference of international cyber security to other topics of specific government interest is that governments are not the only actors in the matrix of power: non-state actors, both private companies and the civil society, hold enormous influence in international cyber security and can themselves be active along all three faces of power.

This is particularly clear when looking at the most fought-over part of international cyber security – the field of Internet governance. In many ways, the power struggle within international cyber security is concentrated within this field, for although Internet governance can be considered to primarily be an "agenda setting" device and therefore a "second face" of cyber power, it substantially touches on the "first" and "third face" as well. For many, Internet governance is no less than the conceptual battlefield upon which the future of cyberspace will be decided.

3. Ruling the Domain: Internet Governance

Cyberspace only exists within parameters constructed and regulated by human beings. These parameters have, until now, not been created directly by governments, but have rather arisen in a bottom-up process that is often referred to as the self-regulation of the Internet. The process is often transcribed as "Internet governance", which has been defined as

> "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet."[15]

This very wide-ranging formulation means that Internet governance is responsible for setting the "rules" of cyberspace, such as how routing functions and how DNS is handled, or indeed what protocols are followed. These rules and norms are not so much laws within the legal sense as they are akin to "physical laws" in other domains, such as the law of universal gravity or Archimedes' principle – they are, in effect, unbreakable. At least, that is, until they are changed.

The key to understanding Internet governance is the "multi-stakeholder approach", which has been tacitly (but never explicitly) defined as being the interplay of governments, the private sector and the civil society in managing the world's Internet resources. This acknowledgement of the strength of non-state actors (and its implied equality with governments) has long irritated countries who consider government to be the natural supreme power. It is, however, simply an expression of reality – Internet governance remains largely a non-state affair.

Internet governance can be subdivided into two domains: the technical domain and the policy domain. The technical domain predominantly consists of volunteers from the private sector and civil society, and it can be described as largely "ad hoc". One of the most important organizations is the "Internet Engineering Task Force" (IETF), which has, since 1986, developed many of the key software protocols and technical fixes the Internet depends upon today. The IETF is famously anarchic, not having any official laws, membership criteria or indeed much more than a basic organization. The members of the IETF "reject Kings, Presidents and voting. We believe in rough consensus and running code."[16] Normally meeting three times a year, the 300 to 1,300 software engineers do not vote on proposals, but hum. Whichever group is perceived to have "hummed louder" carries the (non) vote.[17] There are other, more organized groups, such as the "Institute for Electrical and Electronics Engineers" (IEEE), but the approach is largely always the same: engineers come together in a "bottom-up" (and largely completely volunteer) process with absolutely minimal governmental influence. The IEEE has over 350,000 members and addresses issues regarding connectivity (such as Bluetooth, Wireless and broadband), and anyone can basically join the IETF. Groups such as the IETF and the IEEE can justifiably claim to have built the Internet, one protocol at a time. Governments, at best, have played a supporting role in the process.

The policy domain of Internet governance is relatively more organized. ICANN, the "Internet Corporation for Assigned Names and Numbers" is the one organization that comes closest to having an assigning, coordinating or regulating function (and especially a policy function) on the Internet. ICANN is a nonprofit public-benefit corporation according to the laws of the US State of California, and is based at the University of Southern California. Its purpose is to "coordinate, at the overall level,

14 For an altogether different take on the ways and means that states have in securing non-state cooperation ("co-opt, coerce or convince"), see Alexander Klimburg, "The Whole of Nation in Cyberpower", Georgetown Journal of International Affairs, Special Issue, 2011.

15 WGIG,"Report of the Working Group on Internet Governance", Château de Bossey, June 2005, p. 4, http://www.wgig.org/docs/WGIGREPORT.pdf.

16 Attributed to Dave Clark, for instance in Paulina Borsook, "How Anarchy Works – On location with the masters of the metaverse, the Internet Engineering Task Force", Wired.com, October 1995, http://www.wired.com/wired/archive/3.10/ietf.html.

17 The IETF is, in its very existence, "unofficial" – it does not legally exist, and is officially part of the Internet Society (ISOC) – itself one of the "founding organizations" of the Internet.

the global Internet's systems of unique identifiers."[18] Founded in 1998 on the basis of pre-existing technical organizations, ICANN was the direct result of President Clinton's promise to move the Internet out of the government structures and to open it to the public and to private commerce. Under a contract with the US Department of Commerce, ICANN was to "manage Internet names and addresses," a relatively innocuous-sounding mission encompassing three of the most vital functions of the Internet: the allocation of Internet Protocol number resources for individual computers or machines, and directly corresponding to these, Domain Name Service (DNS) "names," and the allocation of the so-called Top Level Domains (TLDs) to registries which assign these identifiers to individual users and organizations across the globe. Taken together, these three functions represent a considerable segment of Internet functionality.[19] ICANN has grown with the Internet – from a marginal budget in 1999 to USD 60 million in 2010 to over 200 million in 2014. Its nature has changed considerably as well. On the one hand, governments have shown increasing interest in the formative work of ICANN, and its associated Government Advisory Council (GAC) has become especially active, although it does not officially have a veto over proceedings. While ICANN was "released" from US government control in October 2009, the US government still retains extra influence, more than other countries represented on the GAC.

The purported extra US influence on ICANN – which ranges from "marginal" to "strong" depending on viewpoint – has long been a rallying cry for a number of countries keen on breaking the supposed US dominance over this essential function. In particular, the International Telecommunications Union (ITU) has also shown considerable interest in assuming this role.

As an UN-agency (which functions largely independent of the UN Organization), the ITU has played a key role in many of the UN initiatives on cyberspace. It has also been the focus of a number of countries' attempts to "wrestle control "of DNS away from ICANN, a process that gathered speed under the ITU-T 69 Resolution in 2008 and is backed by many Arab states, Iran, Russia, China and clearly supported ITU Secretary General Touré. As an overall statement, it can be said that this core group is united in pushing for an intergovernmental control over the Internet (meaning at least control over DNS), rather than leaving it within the current multi-stakeholder model.

A recent high-water mark of this struggle was the seminal ITU WCIT conference held in December 2012 in Dubai. In this conference, which has also been described as being the "Internet Yalta"[20] of its time, a number of nations – especially in Africa and South America – backed a long-standing Russian initiative to bring ITU closer into Internet governance. This proved to be such a decisive issue that – for the first time in ITU's 140-odd year history – the delegates failed to agree on the basic document (the ITRs)[21] up for discussion, and the US and most OECD nations walked away from the agreement. However, most of the world's governments did sign the new ITRs, effectively leading to a disastrous showdown of the "West against the Rest".

There are a number of potential reasons why this confrontation could be an attractive prospect to the "cyber sovereignty" countries. The first is a rather basic wish to take the management of DNS root "out of the hands" of the US government. This is often argued on the moral (and technically largely incorrect) basis that it is "outrageous that the US could disconnect any country in the world at will" – effectively implying that this represents a "first face" (coercive possibility) of US cyber power.

A second goal is probably much more oblique. The cyber-sovereignty advocates (in particular Russia) have repeatedly tabled a number of international proposals aimed at creating a "code of conduct" that would, in particular, facilitate cross-border cooperation in combating "terrorism" – probably with an uneasy eye towards the role of social networks played in the Arab revolts. Some observers consider the true goal of the cyber-sovereignty advocates is to not only have an international agreement on "cyber crime and cyber terrorism", but also to empower the body that actually controls DNS to function as an effective enforcer of these rules. This would mean that any government could not only filter "criminal content" (or "hostile information") at its own digital borders, it could demand that certain content or activity be subject to a global "notice and take down"-brief, in effect enforcing a global censorship regime.

Why would this be so important a goal to authoritarian regimes? As was pointed out in the beginning of this essay, most of these countries tend to have a much more radical view of the historical importance of the Internet and information in general. Unlike for most OECD countries, "regime stability" is by far the most important criteria in their security assessment. This is enabled not only by the ability of governments to combat hostile content, including e.g. separatist or religious websites, but also their ability to influence the all-important "preference setting" of their respective populations. And one preference that is deeply annoying to authoritarian governments is the contention that government may not be the only, let alone most important, actor – as is defined in the multi-stakeholder approach. Those governments are convinced that the civil society actors are simply proxies for Western interests, and that the private sector has its own agenda to push.

These views are at least half-right. The influence of the private sector on Internet governance is steadily growing, even if not at the same speed as government influence. Like governments, there are different goals among different industry sectors – the traditional telecommunication companies, for instance, are pushing for a share of the profits that Google or Amazon make via their infrastructure, while the traditional movie studios and

18 See, for instance, ICANN, Bylaws, as amended 11 April 2013, http://www.icann.org/en/general/bylaws.htm.

19 DNS in effect functions as the telephone book of the Internet, converting IP numbers into website addresses. IP addresses (and their corresponding DNS entry) are often clustered and managed under specific TLDs. The 'generic Top Level Domains' (gTLD) include all Internet addresses that are no-geographic and e.g. end with .com, .org, or .info. National domains are known as 'country code Top Level Domains' (ccTLD) and, for instance, end with .de, .fr, or .uk.

20 For a commentary on the event, see Alexander Klimburg, "The Internet Yalta", Commentary for the Center for a New American Security, February 2013.

21 The International Telecommunication Regulations have historically been the principle agreement on operative issues in telephony, such as the connection and billing of international phone calls. They had never previously included any Internet-related issues.

music labels are aggressively pursuing an anti-piracy strategy worldwide, lobbying for legislation (such as the infamous SOPA-PIPA bill) that would also, according to detractors, directly impact civil rights. Indeed, a few measures popular in some industry segments are not too dissimilar with proposals by authoritarian governments, and some interesting alliances have already been formed. For instance, at WCIT 2012 in Dubai, one of the factors that may have caused the OECD nations to lose the African block to the "cyber-sovereignty" faction was the persistent lobbying of telecommunication operators, who reinforced notions that the Internet was simply a new form of imperialism, with most of the gains accruing to globally-dominant American companies (rather to them).

4. Quo vadis, Cyber?

Predicting the future of cyberspace is a thankless task. Since 1999, a large number of predictions[22] have been made, and, while most have not panned out as predicted within their relative timelines, the overall trends they draw have proven to be accurate in substance. Still, second-order effects of those identified trends are nearly always in the realm of pure speculation and largely dependent upon the preconceptions of the observer.

Most observers would agree that the future of the Internet – and thus the future of cyberspace as a domain for military activity – will largely depend on what form Internet governance takes. WCIT 2012 may have set the tone for repeated attacks on the definition of "multi-stakeholder". This attack has been significantly reinforced with revelations regarding US espionage, made over the summer of 2013 by a former NSA contractor. Together, these trends all point to a possible "showdown" at what could be the most important meeting in Internet governance history: the UN-sponsored World Summit of Information Society (WSIS) to be held in 2015. While there is a small possibility that WSIS will be fractured, downgraded or even delayed, it is a good point from which to speculate on further developments of the global Internet. In essence, four large scenario groups are probably the most likely, although each of these scenario groups has detailed scenarios within, which can differ greatly from each other.

4.1. "Government Returns": This scenario group has one thing in common – the transfer of the global DNS to an international body and the de facto end of the multi-stakeholder approach. There are a large number of sub-scenarios here, depending on the interplay in particular between the United States and possible overall UN reform, however, the outcome of the "median" scenario is largely standard: government asserts its primacy in all aspects of Internet governance. Or nearly all – the "technical" Internet governance domain – composed largely of volunteers – does not transfer smoothly in this new arrangement. While some engineers are happy in accepting the primacy of the UN in developing technical standards, many are not, and they effectively go underground – turning their energy on developing non-approved standards. In this scenario, the increased connection of the management of DNS with law enforcement cooperation means that there is an initially strong decrease in "petty" cybercrime – i.e. direct against the average user – but serious cyber espionage does not noticeably decrease, although state-to-state agreed "norms of behavior" limit the risk that the espionage may accidently spill over into actual conflict or war. However, the technical Internet governance dimension has increasingly turned its focus towards privacy, and the standards they develop are increasingly at odds with the global Internet – leading to the development of a largely separate (and often criminal) "Dark Net". Similarly, anti-authoritarian movements and hacker-collectives are greatly empowered in this scenario group, and their ability to cause serious damage rises constantly. "Cyber-terrorism" – in terms of destruction of lives and property rather than political agitation – becomes a constant reality.

4.2. "Triarchy": In this scenario group, liberal democracies compromise on an "internationalization" of ICANN, meaning, among other things, that the government role is enhanced within the multi-stakeholder approach. The specifics of the scenarios within this group vary widely, depending on the specifics of the "grand agreement", but in effect they all amount to a reinterpretation and "ordering" of the multi-stakeholder approach, with governments receiving some official veto powers, while at the same time the private sector and civil society components would be greatly reformed and participation reduced to much smaller number. The multiple variants make it difficult to make any predictions on developments in this scenario group, except for one: the likelihood of tension between those who are "in" the present process, and those who feel excluded from it. Also, the possibility of co-opting the most important actors of any individual category means that certain initiatives could become very difficult to resist. Depending on the balance between the different stakeholders, it is possible that some business and government interests could overlap to create a strong momentum for a fundamental redesign of the Internet – a "next generation network" that, among other things, would put an end to relative anonymity of today's Internet users.

4.3. "Warring Webs": In this scenario group, the UN meetings of 2015/2016 lead to a fundamental break between the "cyber-sovereignty" advocates and those promoting "Internet freedom", with a number of countries announcing their desire to manage their own DNS roots and therefore, in effect, their own Internets. Depending on the specifics of the relative scenarios within this group, the fragmentation of the Internet is either relatively minor – with only a couple of countries such as Russia and China opting out – or extreme, with multiple, more or less equally large Internet-blocks competing with each other. Overall, even the most minor scenarios of

22 While a large number of different studies and surveys exist, the 2009 ISOC study is a good example of a highly technology-focused view (see Internet Society, "Internet Futures Scenarios", Internet Society, 6 October 2009, http://www.internetsociety.org/sites/default/files/pdf/report-internetfutures-20091006-en.pdf. For a more military take, see Jason Healey, "The Five Futures of Cyber Conflict and Cooperation", Atlantic Council Issue Brief, 2012, http://citizenlab.org/cybernorms2012/cyberfutures.pdf.

"net fragmentation" see a greatly increased amount of geopolitical tension in cyberspace, with espionage attacks and preparations for all-out warfare blending together in a seamless conflict area of constant "war of the webs". This geopolitical tension is somewhat offset by a marginal decrease in cybercrime, as the new borders and alliances in cyberspace makes global cybercrime more difficult. At the same time, the effective freeze of the free movement of ideas and news means that globalization – at least as a cultural quality – goes into reverse.

4.4. **"Muddling On":** In this scenario group, not much seems to change. The Internet muddles on, security remains an afterthought, and the development of standards and services continues at light-speed. Most scenario variants here revolve around the occurrence of specific geopolitical events, such as crises between individual countries, or the continuing spying and surveillance scandals. In both cases, the increased insecurity of the average consumer may prompt a drive towards commercial "walled gardens" that seek to simplify and secure the user experience, reducing the Internet to a series of apps, or even less. This trend is somewhat offset by the burgeoning "Internet of Things" that requires a certain amount of interconnectivity to be successful and is especially conducive to "generative" technology. This continuation of the rapid technology development means that cyber-attack options will continue to greatly outstrip defense options, encouraging concepts such as resilience and redundancy instead. Similarly, the unceasing media coverage on cyber espionage and, increasingly, cyber activism/terrorism means that there is a higher awareness in the population for the geopolitical dimension of cyber security.

As said previously, all attempts to look into the cyber crystal ball will be completely contingent on the observer's point of view. Equally, the devil is in the details – some of the scenarios within the individual groups differ starkly from each other in outcome, even if they have been assigned the same scenario group. A persistent theme in those groups, as well as this essay as a whole, is the difference in perception of the value of information in general as well as the role of the Internet in particular. The views and aims of liberal democracies and authoritarian governments do have some commonality, but in essence are so very much divergent that, in the view of this author, they are incompatible with each other on a very basic level. The main difference between any "liberal democracy" – including those outside of the OECD – and an "authoritarian state" is the overriding focus of the latter on regime stability, to the detriment of all other considerations. That also means that liberal democracies are particularly challenged when engaging with those nations on such issues as Internet governance – for these issues may very well be considered as "existential" issues for an authoritarian regime, and something that is worth a maximum level of effort. It can be doubted that most liberal democracies see the stakes as being quite so high. But they should.

Cyber Defence – eine nationale Herausforderung

Walter J. Unger*

Abstract: Facing the increasing dependence on cyber infrastructures and vulnerability of the current information society through cyber attacks, this article defines various risks within cyberspace, potential scenarios and challenges of such an attack, as well as in the context of international law and international humanitarian law. The article focuses on questions of responsibility – getting more complex given the non-governmental aspects of cyberspace –, constant protection of critical infrastructure and Europeanization of those aspects which are as relevant as Austria's role, implementing the EU's policies. Finally, it discusses the tasks of the Austrian Armed Forces within cyberspace in the context of defending the sovereignty of Austria in case of an attack.

Keywords: Informations- und Kommunikationstechnologie, Infrastrukturschutz, Internetkriminalität, Internetsicherheit; Information and communication technology, security of infrastructure, cybercrime, cybersecurity.

1. Einleitung

Der Cyberraum[1][2] (englisch Cyberspace)[3] ist jener virtuelle Raum, der durch die Vernetzung von Computern entstanden ist. Derzeit sind bereits mehr als zwei

* Mag. Walter J. Unger, Oberst des Generalstabsdienstes. 2006-2008 Leiter der Interministeriellen Arbeitsgruppe Strategie „IKT-Sicherheit", 2009 Leiter der Abteilung IKT-Sicherheit, seit Mai 2013 Leiter der Abteilung Cyber Defence & IKT-Sicherheit im Abwehramt im Bundesministerium für Landesverteidigung und Sport.

Der Autor dankt Frau Ella-Maria Moritz für ihre wertvolle Unterstützung.

1 Gem. BKA, Österreichische Strategie für Cyber Sicherheit, (ÖSCS), Wien 2013, S. 21 ist der „Cyber Raum der virtuelle Raum aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab. Dem Cyber Raum liegt als universelles und öffentlich zugängliches Verbindungs- und Transportnetz das Internet zugrunde, welches durch beliebige andere Datennetze ergänzt und erweitert werden kann. Im allgemeinen Sprachgebrauch bezeichnet Cyber Space auch das weltweite Netzwerk von verschiedenen unabhängigen IK-Infrastrukturen, Telekommunikationsnetzen und Computersystemen. In der sozialen Sphäre kann bei Benutzung dieses globalen Netzwerkes zwischen Individuen interagiert werden, Ideen ausgetauscht, Informationen verteilt, soziale Unterstützung gewährt, Geschäfte getätigt, Aktionen gelenkt, künstlerische und mediale Werke geschaffen, Spiele gespielt, politisch diskutiert und vieles mehr getan werden. Cyber Space ist ein Überbegriff für Alles mit dem Internet verbundenes und für die verschiedenen Internet Kulturen geworden. Viele Staaten betrachten die vernetzte IKT und die unabhängigen Netzwerke, die über dieses Medium operieren als Teil ihrer Nationalen Kritischen Infrastrukturen".
Vgl. auch Cyber-Sicherheitsstrategie für Deutschland, Bundesministerium des Inneren (Stand: Februar 2011), S.14.

2 Der „virtuelle" Raum beginnt und endet im physischen Raum und umfasst Endgeräte, Netzwerkgeräte, Leitungen,...