TNO

STRATEGY & CHANGE

THE FUTURE OF CYBERSECURITY

THE HAGUE CENTRE FOR STRATEGIC STUDIES AND TNO

TNO

STRATEGY & CHANGE

THE FUTURE OF CYBERSECURITY
THE HAGUE CENTRE FOR STRATEGIC STUDIES (HCSS) AND TNO

PAPER Nº 2011•04
ISBN/EAN: 978-94-91040-29-0

Author: Sacha Tessier Stall

This publication is also part of the Security Foresight Programme. It has been made possible by:

TNO innovation for life
THALES
Capgemini
IG.TECHNOLOGY.OUTSOURCING
Ministerie van Buitenlandse Zaken
GRANARIA HOLDINGS

Graphic Design: Studio Maartje de Sonnaville, The Hague
Print: Koninklijke De Swart, The Hague

HCSS, LANGE VOORHOUT 16, 2514 EE THE HAGUE
T: +31 (0)70-3184840 E: INFO@HCSS.NL
W: STRATEGYANDCHANGE.NL

THE FUTURE OF CYBERSECURITY

THE HAGUE CENTRE FOR STRATEGIC STUDIES AND TNO

TNO

STRATEGY & CHANGE

The TNO and *The Hague* Centre for Strategic Studies (HCSS) programme Strategy & Change analyzes global trends in a dynamic world affecting the foundations of our security, welfare and well-being.

The programme attempts to answer the critical question: what are the policies and strategies that must be developed to effectively anticipate on these emerging challenges?

Strategy & Change provides both a better understanding and feeds the agenda for a sustainable future of our society.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cyberspace is both the playground and the battleground of the future. The use of information and communication technologies (ICT) is expanding across the globe and becoming increasingly central to societies. This growing cyber dependence, evident among both public and private actors, is making ICT ever more attractive targets for actors of all types looking to exploit, disturb or destroy competitors and opponents.

This Future Issue examines the future of cybersecurity as envisioned in the foresight literature. That future is one where cyberdependence continues to grow, even as cyberspace becomes more and more vulnerable. It is one in which non-state actors and public-private partnerships are increasingly central to the execution of – and to protection against – cyberattacks. And it is a future in which critical national infrastructures, such as electricity and telecommunications grids, are ever more susceptible to disruption.

Driving cybersecurity changes will be the security awareness of public and private actors. Already acutely conscious of the risk they face, they will continue to seek out ways to insulate themselves from security threats. Any successes, however, will be temporary: technological developments will provide the targeting side with an initial advantage. The targeting side will generally benefit from the power of surprise by applying another new method or approach. At the same time, our increasing dependence on ICT will make the payoff or impact of a successful cyberattack skyrocket.

This will have major implications for national and international security. The very definition of warfare will evolve to include cyberattacks, with virtual assaults becoming grave enough to provoke not only cyber (counter) attacks but also kinetic (conventional) responses[1]. As cyberattack capabilities become steadily more destructive and more widespread, the incentive for pre-emptive strike will rise. A virtual arms races will become

more common. This will lead to a strengthening of calls for an international cyber arms control regime or for laws on armed cyber conflict.

The pool of cybersecurity literature is young and relatively shallow, but some things are clear: ICT will become increasingly ubiquitous, cyberspace will become more and more vulnerable, and governments will have no choice but to enter into deep partnerships with the private sector.

It is these and other – sometimes surprising – findings that this Future Issue sets out to analyze.

INTRODUCTION

Use of information and communication technologies (ICT) permeates almost every facet of our everyday existence, from social interaction to financial transactions. For most people, ICT security is about protecting personal information or keeping PCs running fast and malware-free (and indeed almost everyone has been the victim – knowingly or not – of some sort of cyberattack).

Few realize, however, just how dependent their societies are on ICT and ICT infrastructures, and how frail these systems can be. Today, a major ICT failure could disable an entire electricity grid or cripple a national telecommunications network, either of which could cause significant damage and loss of life. Combined with a kinetic attack, a virtual assault has the potential to bring even the most advanced society to its knees.

Cyberspace today is expanding faster than our ability to defend it. Cyberspace is defined as ICT systems, networks and the information contained within these systems and networks, whether online or offline. Cyber security is defined as the uninterrupted functioning of these systems. Cyberattack capabilities are spreading rapidly among both states and non-state actors (such as (h)activists, terrorist groups and organized crime). At the same time, ICT-based functions are growing ever more interdependent, increasing the risk of 'cascade' or 'domino' failures.

This Future Issue analyzes the body of foresight literature dedicated to the future of cyberspace security. To do so it examines the following, as described in the studies surveyed:

- **Parameters**: the aspects of ICT security most likely to evolve over the coming decades
- **Drivers**: the reasons behind changes expected in the Parameters

- **Security Implications** of evolutions in cybersecurity

These are analyzed below. But first, a few words about our methodology, and on the state of the cybersecurity foresight debate.

CYBERSPACE, THE UNDISCOVERED COUNTRY

This study applied the HCSS *Metafore* methodology to analyze foresight studies on the future of cybersecurity. These were obtained through a three-stage search protocol: Phase 1 involved scanning the HCSS *Metafore* database for cybersecurity foresight studies. In Phase 2, this search was extended to external databases, using multiple search terms (e.g., 'future', 'ICT', 'cyber security', 'cyberspace'). Finally, Phase 3 involved a direct survey of foresight organizations to net any studies that might have slipped through the various databases.

Foresights included in this study meet three criteria. They:
A) deal specifically with ICT security ('cybersecurity')
B) contain a concrete forward-looking element
C) were published in the last 15 years

This research protocol yielded a set of over 50 usable studies – by no means overwhelmingly large, but sufficiently rich and internally variable to warrant in-depth analysis. These English-language papers were published by a range of organizations encompassing academia, government, the private sector and civil society, and thus contain several perspectives. However, with countries like China and Russia among the most important cybersecurity actors, the exclusion of non-English sources must be considered a weakness of the dataset used herein. The foresight studies used are listed in Appendix II.[2]

As is evident from Figure 1, there is a clear upward trend in the number of cybersecurity studies, with 2007 a watershed year. Unfortunately, the foresight community seems to have suffered a bout of 'presentism,' only becoming earnestly interested in the issue *after* it had become important. Indeed, the past few years have witnessed a steep increase in reported financial losses (see Figure 2), a drastic proliferation in new malware

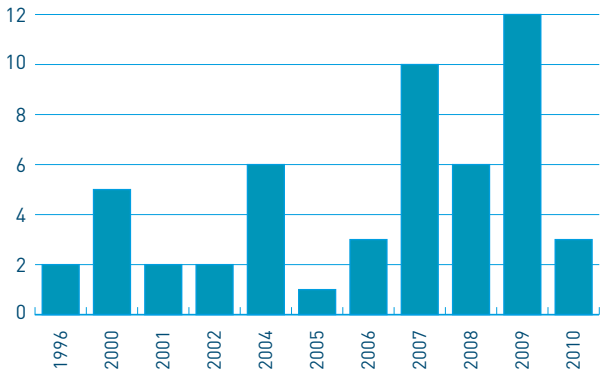

FIGURE 1. PUBLICATION OF FORESIGHT STUDIES

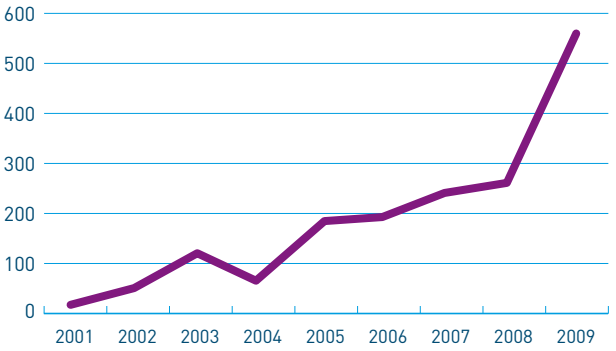

FIGURE 2. US REPORTED FINANCIAL LOSSES (IN MILLION USD)[3]

signatures (see Figure 7), and a high-profile international cyberattack against Estonia. Hence the period 2007-2009 saw an average of 9.3 studies published per year, more than three times the 2000-2006 average of 2.83. In other words, the foresight community noticed the increasing importance of cybersecurity – instead of anticipating it.

Together, research institutes (including university-affiliated centers) and private business account for approximately half of the reports published

over the last 15 years, with government, NGOs, the military and independent think-tanks splitting the rest (see figure 3).

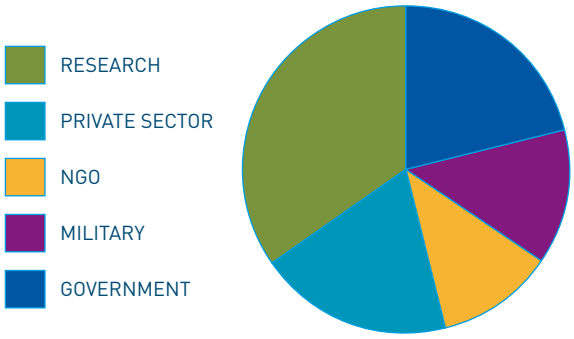

FIGURE 3. SOURCES PUBLISHING ON ICT SECURITY

This overall distribution, however, obscures a highly significant trend (see Figure 4): that the centre of gravity of cybersecurity foresight is shifting away from the academic and contemplative research model toward the policy and business communities.

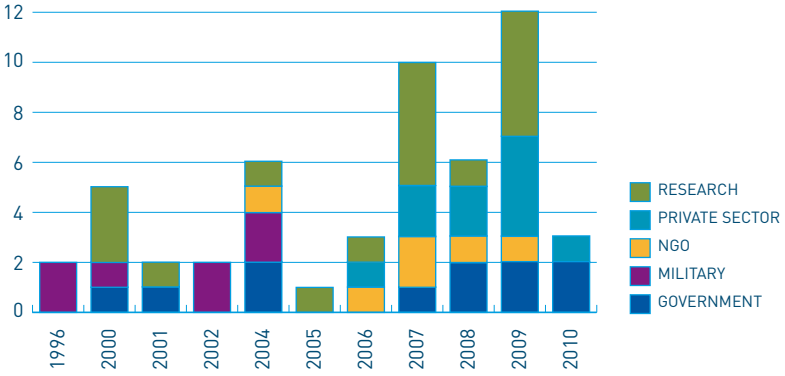

FIGURE 4. CYBERSECURITY PUBLICATIONS BY SOURCE BY YEAR

Indeed, whereas governments did not pay much attention to cybersecurity foresight until 2006, by 2009 they had become one of the main producers of such studies[4]. This can be linked not only to the general upward trend in cyberattacks, but also to their increasingly obvious implications for national security. After Estonia in 2007, it was Georgia's turn in 2008, and Kyrgyzstan's in 2009 to bear the brunt of alleged Russian cyber attacks: the incidents confirmed that the era of interstate cyber operations had begun. Moreover, the public reports about state (or state sponsored) intelligence collection using cyber exploitation means increased considerably over the same period: Moonlight Maze, Gh0stnet (2009), Operation Aurora (2010). And, last but not least, the Stuxnet worm in 2010 seems a clear example of Cybotage, an attempt to sabotage the uranium enrichment plant in Natanz, Iran and the Iran nuclear program.

Similarly, since 2008 the number of foresights produced by the private sector has increased dramatically, reflecting a growing concern about cyberspace vulnerabilities.

In other words, cyber threats are increasingly seen not as an abstract future problem, but as a clear and present risk with concrete implications for both the private and public sectors.

Nevertheless, it bears mentioning that the cybersecurity foresight literature, in addition to being recent and sparse, is also of relatively poor quality. Most of the texts analyzed for this study have a distinctly intuitive, rather than analytical, flavor. Of course, foresight by definition entails speculation – but few papers have achieved the necessary balance of current analysis and robust forecasting. Exceptions to this rule include the Project for Defense Alternatives' *Arms Control in an Age of Strategic and Military Revolution*, the 2008 IIEE Computer Society *Information Assurance Technology Forecast,* and Robert A. Miller and Daniel T. Kuehl's *Cyberspace and the 'First Battle' in 21st-century War.*

I) KEEPING TRACK AND KEEPING UP: THE EVOLUTION OF OUR CYBERDEPENDENT WORLD

The foresight community has identified five essential parameters that will characterize the cybersecurity landscape over the coming decades. These are: *ICT ubiquity; the degree of security in cyberspace; responsibility for cyberspace governance; sources of cybersecurity threats;* and *cyberattack targets.* These are discussed below.

1. ICT UBIQUITY: NOWHERE TO GO BUT UP

Unsurprisingly, there is a robust consensus within the foresight community that ICT will only become more ubiquitous (omnipresent) (see Figure 5). All of the studies assessing this parameter predict both the geographical expansion of cyberspace (reaching more and more communities), and its functional growth (becoming increasingly central to these societies).

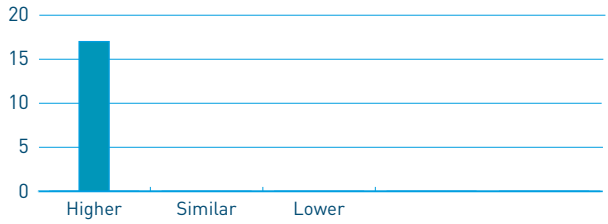

FIGURE 5. ICT UBIQUITY IN THE COMING YEARS – NUMBER OF FORESIGHT PREDICTIONS

There is today a significant 'cyber-divide' between the developed world, in which the public and private sectors are becoming increasingly cyber-dependent, and part of the developing world, where ICT use is still in its infancy. This gap, however, is narrowing with cyberspace becoming ever more vital to countries across the globe. From 2000 to 2009 the number of Internet users in Africa, Asia and the Middle-East jumped 1,392.4%,

545.9%, and 1,648.2%, respectively.[5] Cyberspace penetration is progressing on other levels as well.

This trend will persist for the foreseeable future, as falling costs make this technology more and more accessible. One foresight study even predicted a worldwide computer literacy rate of 90% by 2025.[6] These falling costs, combined with technological progress, make today's cutting edge tomorrow's standard. As these technologies become more accessible, more powerful and more portable – Moore's Law predicts a doubling of computing power per microprocessor every two years – they will increasingly be incorporated into everyday consumer goods, and devices will become increasingly multifunctional (compare today's smartphones to the mobile phones of five years ago).

2. DEGREE OF SECURITY IN CYBERSPACE: INCREASINGLY RISKY BUSINESS

The other consensus is that cyberspace will become increasingly vulnerable: no one in the foresight community deems total security a realistic objective (see Figure 5). It should be noted, however, that as threats are the central focus of the cybersecurity literature, the dataset used for the present analysis exhibits a 'doom and gloom' selection bias that likely emphasizes risks and neglects solutions and progress.

Still, it is clear that as cyberspace grows it will become ever more complex and dependent, developing new vulnerabilities while at the same time becoming too large for 'defenders' to adequately patrol. This, combined with the spread of hacking abilities, means that chinks in its armor will likely appear faster than they can be repaired. As one study put it, malicious actors 'are increasing their skills both to stay one step ahead of security professionals and to craft even more sophisticated attacks'.[7]

The foresight literature makes it clear that as cyberspace becomes more vulnerable, it will become the battleground of choice for actors of all types. Indeed, the virtual plane has something for everyone. To individual hackers, cyberattacks offer the possibility of easy enrichment through data theft. For unscrupulous corporations, they hold the key to a gold mine of information on clients and competitors – not to mention regulators, law enforcement agencies and intelligence services. To small nations and non-

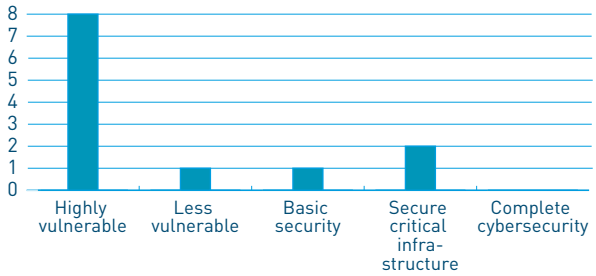

FIGURE 6. ANTICIPATED DEGREE OF SECURITY IN CYBERSPACE – NUMBER OF FORESIGHT PREDICTIONS

state actors (including terrorist groups), they offer the ability to cripple militarily superior opponents. For great powers, cyberattacks constitute both a new way to coerce weaker countries, as a force multiplier and as a weapon for use against major adversaries – one less likely to lead to all-out war. And finally, cyberattacks give their attackers the ability to remain anonymous or to make their identities known worldwide (and any position in between) – a priceless choice whether in terrorism, crime, or military operations.

The foresight community is practically unanimous that critical infrastructure, and in particular process control systems (including SCADA - Supervisory, Control and Data Acquisition systems) will be increasingly vulnerable.[8] As one analyst put it, in the event of cyberwarfare opposing two nation-states 'neither would emerge from the first day of combat with their digital nets intact. And both sides would likely suffer substantial damage to their national infrastructures'.[9]

As Figure 7 shows, malware signatures are being created at an exponential pace. With network convergence on the rise, various types of information will increasingly travel in common streams toward common pools.[11] No matter how many lifeguards are posted, information theft will become easier and its payoff will grow. Malware creation is therefore likely to continue unabated.

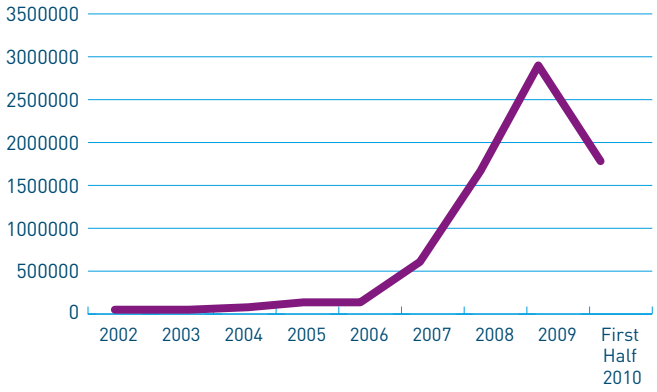

FIGURE 7. NEW MALWARE SIGNATURES[10]

3. ACTORS RESPONSIBLE FOR CYBERSECURITY: MIX AND MATCH

The question of who should be in charge of countering cybersecurity hazards has received relatively little attention. Government and nongovernmental studies alike tend to assume – rather than predict – that primary responsibility will fall to state institutions (see Figure 8), while at the same time neglecting to describe how these should be structured.

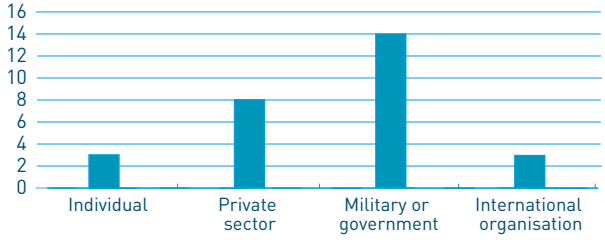

FIGURE 8. ACTORS RESPONSIBLE FOR CYBERSECURITY – NUMBER OF FORESIGHT PREDICTIONS

There is one other point on which most analysts agree: ensuring cybersecurity will increasingly require public-private partnerships and international collaboration. This is already understood by governments

worldwide. In February 2010, US Director of National Intelligence Dennis Blair put it starkly: 'We cannot protect cyberspace without a coordinated and collaborative effort that incorporates both the US private sector and our international partners'.[12]

As network convergence continues and dual-use infrastructures (privately operated elements used by both government and the private sector) become more widespread, the public and private 'cyberspheres' will increasingly overlap. The need for regulation, law enforcement and a holistic picture will make government involvement ever more essential, but no state will enjoy the total access and control necessary to patrol its entire patch of cyberspace: even today, approximately 90% of the US national security infrastructure is in the hands of the private sector.[13] In the future, defense and law enforcement agencies will have to collaboratively work with the private sector in more and more fields, for instance in fraud investigations.[14]

The need for public-private partnerships will also be driven by the pace of change in cyberspace. Legislation and policy are typically a few steps behind the technological status quo. Governments will only be able to keep up if they are in frequent contact with the actors most aware of trends and vulnerabilities – often firms specializing in cybersecurity or those handling sensitive data, such as banks.[15] Collaboration with smaller private actors, such as individuals and online communities, will also have to be part of any effective strategy. As one study pointed out, today 'individual PC users have more capacity at their fingertips than NASA had with the computers used in its first moon launches. Individuals and small groups… will plan, mobilize, and accomplish tasks with potentially more satisfying and efficient results than their governments can deliver.[16]'

If public-private partnerships will be essential to cybersecurity, so too will international cooperation. The 'deterritorialization' of criminal or terrorist networks will require fast and prompt coordination and information-sharing among allied defense, intelligence and law enforcement agencies, as will protection against cyberattacks launched by nation-states. This need, long met through informal, ad hoc cooperation, has only recently begun to take institutional shape. In 2008, one year after the cyberattack on Estonia, NATO created a Cooperative Cyber Defense Center based in Tallinn. This raises the question of whether future 'cyber alliances' will simply mirror

military-political blocs (such as NATO and the Collective Security Treaty Organization), or whether cyber defense will develop its own dynamics. Unfortunately, the foresight literature assumes the former and has of yet not seriously considered the latter.

4. THREATS TO CYBERSECURITY: SOMETHING FOR EVERYBODY

If the foresight community is somewhat divided on the responsibility for governing cyberspace, it is still more fragmented when it comes to the responsibility for future cyberattacks (see Figure 9). Significantly, this issue is much more widely discussed than any of the three parameters examined above.[17] The literature predicts that in the long run, it is non-state actors (such as terrorists, 'hacktivist' groups, organized crime and lone individuals) that will pose the direst threats to cybersecurity. While their motives may differ, all will exploit the low cost of mounting a cyberattack and the increasing vulnerability of sensitive information. The attacks on various banks and Mastercard after Julian Assange, the Wikileaks editor-in-chief, was arrested in December 2010, are a case in point.

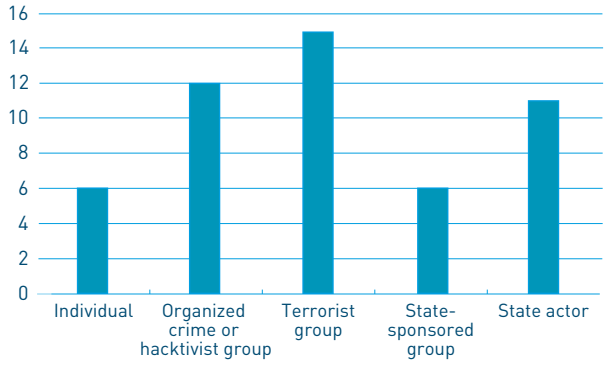

FIGURE 9. SOURCES OF THREATS TO CYBERSECURITY – NUMBER OF FORESIGHT PREDICTIONS

Terrorist groups are identified as most likely assailants. Indeed, the heavy reliance of many societies on their ICT infrastructures, the vulnerability of said infrastructures, and the comparatively low cost of cyberterrorism will combine to make the virtual plane a battleground of choice. With

cyberspace dependence a major feature of modernity, a devastating cyberattack would also carry much ideological weight for a terrorist group looking to make a point.

It should be noted, however, that the foresight community expects increasing cooperation between types of state actors, state-sponsored actors/ cyber mercenaries, non-state actors, individual cyber volunteers, and even the blurring of the distinctions between them. In the words of one study, 'the boundaries between criminal syndicates, terrorist groups, and gangs will continue to disappear. Alliances between seemingly disparate and unrelated organizations should be expected. Physical boundaries will be replaced by electronic and philosophical ones as individuals discover new virtual communities'.[18] This includes social communities (e.g., Twitter) as well.

Still, it will be some time before the capabilities of non-state actors match their ambitions. In the meantime, the foresight literature predicts that it is states that will pose the most serious threats. Cyberattacks offer the ability to achieve one of the most sought-after objectives in warfare: to disable an opponent while maintaining anonymity. Several countries, including the US, the UK, China and Russia, have made cybersecurity a key facet of their military operations. The 2007 cyberattack on Estonia, the most high-profile incident to date, is widely believed to have been orchestrated by groups eather close to or in the Russian government, while China is known to have successfully hacked into the Pentagon's computer system. It is estimated that over half of the countries in the world are developing cyber warfare capabilities; with these expected to become operational within the next 15 years, the possibility of inter-state cyber warfare will be a key feature of the cybersecurity landscape for the foreseeable future.[19]

As noted above, defense against cyber threats will increasingly depend on public-private cooperation. This also applies to the *execution* of cyberattacks. Indeed, the cyberattacks on Estonia, Georgia and Kyrgyzstan were largely, if not entirely, carried out by Russian non-state groups. Though it has of yet been impossible to conclusively demonstrate governmental involvement, the timing, coordination, and scale of these actions strongly suggest a helping hand from above, as well as (in the case of Georgia) an advance warning of the conventional military campaign they were used to

support.[20] Such state-sponsored groups are likely to play a growing role in the cyber conflicts of tomorrow: their use allows the simultaneous exploitation of public and private capabilities, while at the same time affording the sponsoring government a measure of deniability.

Public-private partnerships have received a great deal of attention in the cybersecurity discourse; offensive ones have not, though the policy discourse seems to be rectifying this imbalance. This constitutes a major shortcoming, as cyberoffense will likely have a significant impact on the interaction between public and private actors a few years down the road.

5. LIKELY TARGETS: BEWARE THE DOMINOES

The foresight literature points to critical infrastructures, including SCADA systems, as the most likely targets of cybersecurity threats (see Figure 9). Growing interdependence constitutes a significant threat to the integrity of critical infrastructures: a single compromised system may lead to 'cascade failures,' as those connected to it crash like dominoes.[21] As one study explained, 'in any future conflict, strategic infrastructures will be a major, and perhaps decisive, battleground... [C]yberspace will be the major theater for the conduct of such operations, if only because it offers a fast, relatively inexpensive, and effective way to assail and degrade critical but vulnerable infrastructures'.[22]

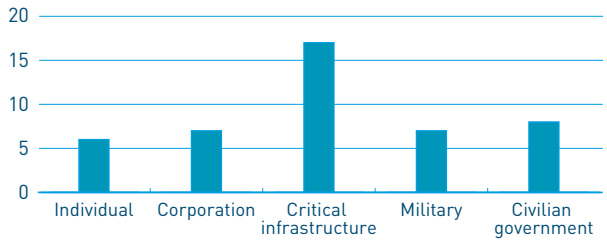

FIGURE 10. ANTICIPATED TARGETS OF FUTURE CYBERATTACKS – NUMBER OF FORESIGHT PREDICTIONS

Dual use infrastructures are not always adequately protected, and will therefore continue to represent a major chink in any cyber armor. Telecommunications, financial networks, and power distribution all depend

on such systems.[23] As this dependence deepens, these infrastructures will become increasingly attractive targets – as will governmental and military ICT and ICT-based infrastructures.

Both states and terrorist groups may target these infrastructures, but, according to one foresight, the latter are unlikely to develop the necessary expertise in the next decade. Absent opportunities to cripple entire countries, they will likely turn their attention to 'high visibility organizations' like large corporations and the media.[24]

Over the coming years, the flow of information will become increasingly concentrated. This will make protected data more and more vulnerable, while at the same time boosting the informational payoff of a successful cyberattack. As a result, individuals and corporations will continue to be targeted by teams of profit-seeking actors – hackers, spammers, identity and credit-card thieves – working together to gain access to sensitive information.[25] This access will continue to be used to steal money, to collect and sell data (such as personal information, intellectual property, industrial and national secrets), and to blackmail states, corporations, and individuals.[26]

II) THE CHANGE BEHIND THE CHANGE: META-ANALYSIS DRIVERS

The foresight literature identifies three drivers that will determine the direction and pace of changes in the realm of cybersecurity. These are: *increasing increasing ubiquity, dependence, and interdependence; technological developments; and security awareness* (see figure 11).

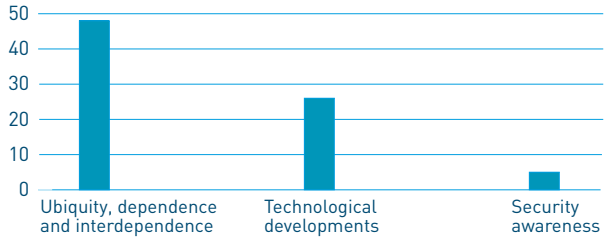

FIGURE 11. DRIVERS OF THREATS TO ICT SYSTEMS – NUMBER OF FORESIGHT PREDICTIONS

1. INCREASING ICT DEPENDENCE AND UBIQUITY

The foresight community has identified the proliferation of prospective cyberattack targets as the main driver of evolutions in cybersecurity. As institutions and individuals increasingly rely on ICT, the number and size of vulnerable components, systems and networks will grow. To use but one example, in 2005 the Project on Defense Alternatives predicted a hundredfold increase in the bandwidth required by the US military alone by 2015.[27]

As explained above, this increasing dependence on ICT will be coupled with growing interconnectivity between systems. Cyberspace will become more and more vulnerable to the 'weakest link' effect, rendering the entire network as fragile as its most vulnerable component. In February 2010, US

Director of National Intelligence Dennis Blair predicted that network convergence would be 'close to completion' by 2015 and emphasized that 'the increased interconnection of information systems and data… poses potential threats to the confidentiality, integrity and availability of critical infrastructures and of secure credentialing and identification technologies'.[28]

Combined, these two trends will make the impact of a successful cyberattack skyrocket – and with it, the incentive for such an attack. Vulnerable networks will include not only those well known to the public (such as the Internet and financial networks), but also less publicly known technologies such as process control, in-car systems and medical appliances.

The ever higher incentive for cyberattack will be matched by the growing number of potential attackers. As mentioned before, falling costs and greater access to education are eating away at the 'cyber-divide' between the developed and developing worlds, and Internet usage in Asia, Africa and the Middle East is rising rapidly. It bears repeating that some analysts predict a 90% worldwide computer literacy rate by 2025.[29] As connectivity spreads (see Figure 12), so will criminal and terrorist networks. It does not take a crystal ball to predict that the Internet 'will continue to be used to foster allegiance to tribes, religions, and ethnic groups', and that the proliferation of violent networks will stretch surveillance and law enforcement resources.[30]

2. TECHNOLOGICAL DEVELOPMENTS: PERPETUAL CAT-AND-MOUSE

As dictated by Moore's Law, computing power will continue to increase exponentially for the coming years. Given this rate of evolution, is it difficult to predict what the technological landscape will look like a few years into the future – but some trends are already obvious. Cybersecurity will experience what could be called the 'seesaw phenomenon,' with one technological development provisionally giving the offense or defense the upper hand, and the next turning the tables.

On the attacking side, new technologies (and the innovative use of old ones) will allow hackers and cybercriminals to launch increasingly complex

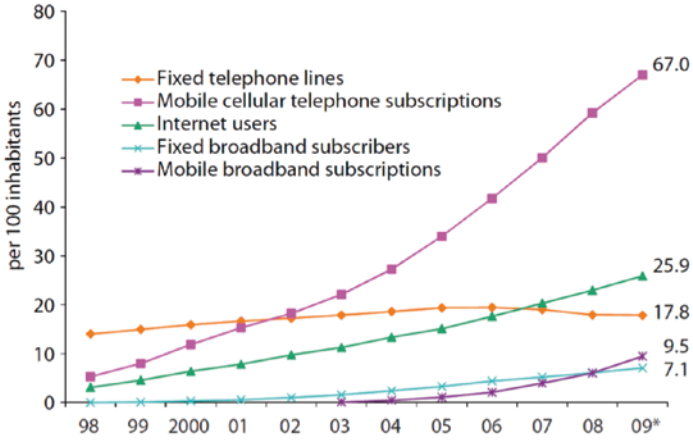

FIGURE 12. GLOBAL ICT DEVELOPMENTS SINCE 1998[31]

and very targeted attacks drawing on several weapons at once. As one foresight put it, 'the days of a single exploit, be it a worm, virus, botnet, spam, etc., are over'.[32] Programmable logic controller attacks (e.g., Stuxnet), CPU-dependent malware, and location-based attacks are just some examples. As the *types* of infection evolve, so too will the *modes* of infection – the means by which malware is made to contaminate systems. Hackers will namely exploit vulnerabilities in cloud computing, mobile networks, smartphones, plug-in media, and even social networks.

On the defending side, meanwhile, the claim of Lawrence K. Gershwin, US National Intelligence Officer for Science and Technology, still holds, in that:

> *'the incremental deployment of new or improved security tools will help protect against both remote and inside threats. Technologies [will] include better intrusion detection systems, better methods for correlating data from multiple defensive tools, automated deployment of security patches, biometric user authentication, wider use of encryption, and public key infrastructures to assure the authenticity and integrity of e-mail, electronic documents, and downloaded software'.*[33]

3. SECURITY AWARENESS

The last key driver is consciousness of the need to improve cyberspace security. Both the public and private sectors are already acutely aware of the gravity of the threats they face, and will only become more so in the coming years. Individual users are much less so. It is the combined and, increasingly, the common agendas of these three sets of actors that will determine the backdrop against which other developments unfold. As these are widely discussed above, they are only summarily described below.

On the public side, governments across the globe are increasingly focused on developing cyber offense and defense capabilities. As mentioned above, the 2007 Internet attack on Estonia raised the international cybersecurity consciousness to a new level and led NATO, for example, to establish a Cooperative Cyber Defense Center. A 2007 foresight study by McAfee estimated at approximately 120 the number of countries developing cyberattack capabilities, with these programs expected to mature within 10-20 years.[34] The United States, the United Kingdom, Canada and Australia have all developed national cybersecurity strategies; The Netherlands is developing a Netherlands Cyber Security Strategy which is scheduled to appear in March 2011. France and Sweden are also improving their ICT infrastructures. China and Russia have made clear that ICT is central to their national security strategies. There are also growing calls for international cyber arms control from many quarters.

With ever larger quantities of protected data at risk, individuals, private organizations and governments also understand the urgency of ensuring cybersecurity. Relevant spending is on a clear upward trend, and the private sector accounts for an increasing share of cybersecurity research. In the midst of drastic budget cuts, the UK government has set aside £650 million for cybersecurity.

Government priorities will increasingly influence cybersecurity R&D, and regulation will continue to define minimum security standards. However, the private sector will maintain its technological leadership. In other words, the ever more symbiotic public-private relationship will reinforce itself and the concern with cybersecurity.

III) SECURITY IMPLICATIONS: THE NEW TELEKINESIS

The changes and drivers described above have clear implications for the 'hard' security landscape of the coming decades. Most important among these are those impacting military doctrine and force structure; cyber arms races and arms control; the involvement of new actors in conflicts; and the incentive for a pre-emptive strike (see figure 13).

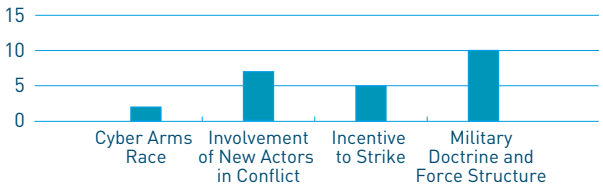

FIGURE 13. 'HARD' SECURITY IMPLICATIONS OF EVOLUTIONS IN CYBERSECURITY – NUMBER OF FORESIGHT PREDICTIONS

1. MILITARY DOCTRINE AND FORCE STRUCTURE

The foresight literature suggests that evolutions in cybersecurity will have the greatest impact on military doctrine and force structure paradigms. In the future, the definition of military conflict will expand beyond 'conventional' warfare. As the cyberattacks suffered by Georgia, Kyrgyzstan, and, especially, Estonia demonstrated, information infrastructures are and will remain key targets in military (and sometimes even political) conflict. But as ICT dependence grows and cyberspace disruptions become more debilitating, cyberattacks will become sufficiently serious to provoke cyber counter attacks and kinetic responses.

Of course, cyberspace dependence will deepen for a reason: ICT will allow for ever greater precision and efficiency, improving the 'kill ratios' of

technologically savvy militaries. The 'information revolution' is designed to allow 'a reduction in the mass and density of armed forces and a corresponding increase in their speed, flexibility, and agility' by improving the information and intelligence position, situational awareness, precision, range, coordination, and support. This in turn will allow forces to 'become smaller and lighter, to operate in a more dispersed fashion, to act with greater speed and agility, and to adapt more rapidly to new circumstances [...]'.[35] States unable to match this technical prowess will compensate by augmenting their kinetic capabilities, growing their conventional arsenals and improving delivery systems.

2. CYBER ARMS RACE AND ARMS CONTROL

The United States military will remain the world's most technologically advanced in the near and medium terms, benefiting as it does from nearly as much funding than the world's other armed forces combined. This will not, however, insulate it from debilitating cyberattack. Geopolitical rivals will continue to develop their own capabilities and therefore pose serious threats to the ICT integrity of the US and its allies. As noted above, a majority of countries are developing cyberattack capabilities, while nations like the US, Russia – and especially, China – already enjoy world-class cyber warfare capabilities and have overtly stated their intention to make them central to their military strategies.[36]

The growing destructive potential of cyberattacks will make cyber arms control an increasingly salient issue, as will ICT parity. As it becomes ever more difficult and expensive to gain the technological upper hand, the incentive for a binding multilateral commitment will increase. A 'real' push for cyber arms control – one originating from major rather than peripheral players – will come when capabilities are at comparable levels, a breakthrough is unlikely, and the cost of arms development is a significant drain on resources. These conditions are already variously met, and calls for international controls are being heard from various quarters – including cyber warfare leaders such as Russia.[37] As a result, the next 10-15 years will likely see significant progress toward cyber arms control.

3. INVOLVEMENT OF NEW ACTORS IN CONFLICT

Also fundamental is the expanding set of actors involved in cyber conflicts. Public-private partnerships will play increasing roles in both the execution of and defense against cyberattacks. Attacking nations may rely on non-state groups to enhance their capabilities and provide cover, while the defense of dual-use infrastructures will require ever greater protection, coordination and regulation by the state.

To poorer or weaker states, the relative ease of acquiring cyberattack capabilities will make this an attractive alternative to WMD development. As one study put it, 'any agency that is willing and able to invest $100 million per year can develop a resilient, world-class cyber-warfare capability within a decade or less'.[38]

Finally, private, independent actors such as (h)activists, terrorist groups, organized crime and individual hackers (acting alone or as groups) will also become increasingly important. They will attack states, individuals and corporations, for various motives but using essentially the same accessible and relatively cheap means. This will put any entity with a direct or indirect public network connection at risk – and therefore make it an actor, however active or passive, in cyber conflicts.

4. INCENTIVE TO STRIKE

The foresight studies examined also make it clear that evolutions in cybersecurity will boost the incentive to strike pre-emptively. Cyberattacks are similar to nuclear weapons in that successful delivery can instantaneously cripple an opponent; they are also highly dependent on vulnerable infrastructures such as space-based assets and information networks. While states will take precautions to retain second-strike capability, this is, in the words of one study, 'a configuration that invites pre-emption'.[39] Indeed, the struggle for cyberspace dominance will be

> *'fought at the beginning of hostilities and probably begun long before… [T]his cyber struggle for mastery will have significant consequences for a nation's ability to deploy, support, and fight, especially in a conflict of short duration aimed at focused and limited objectives. Winning that*

> *future war — defined in Clausewitzian terms as the attainment of strategic political objectives — thus may depend on successfully waging and winning the 'first battle in cyberspace'.*[40]

First-strike cyberattacks will have one or any combination of the following objectives: anticipation (strengthening the information position), destruction or disruption. The direct destruction of physical assets, today beyond the scope of even the most sophisticated cyber warfare capabilities, will be within reach of only the most advanced militaries. The indirect destruction, however, might already have taken its first victims, for instance in the Stuxnet case.

Disruption (the crippling or even hijacking of an opponent's information processing systems), on the other hand, requires comparatively little skill and investment, and has already occurred on scales both large (Estonia) and small (credit card theft). Due to their greater ease, disruptive attacks will be the more frequent, available as they will remain to cyber actors of all types and degrees of sophistication. The plethora of entities capable of launching such attacks will also provide cover for cyber attackers wishing to stay off the radar entirely.

CONCLUSION

When it comes to cybersecurity, the foresight community has been conservative rather than innovative in understanding the new realm. The themes it echoes have changed little over the past decade and a half. The community failed to predict the issue's now central importance, and even today it too often falls prey to 'presentism.' On the whole, the studies analyzed above merely extrapolate from current trends without examining their wider implications – nor do they anticipate necessary paradigm shifts. Few make room for cybersecurity to develop its own geopolitical dynamics, and public-private partnerships are almost exclusively viewed in a defensive (rather than attacking) perspective.

Still, there is consensus around three points. First, ICT ubiquity will continue to grow. Second, cyberspace will become less, not more, secure. Finally, public-private partnerships will be essential to the preservation of cybersecurity. As ICT dependence deepens, it will become ever more crucial to understand these trends.

In conclusion, HCSS wants to present a number of general observations and recommendations to policymakers, also based on other related work[41], on how to devise adequate responses to the challenges posed by the rapidly evolving nature of cyber security:

- Cyber security is subject to constant and rapid changes which require the constant renewal and reassessment of policies and which also produce an ambient vulnerability. In turn, this requires a focus on vulnerability reduction, recovery and resilience. If ICT continues to become increasingly ubiquitous in society at large, these trends are only likely to grow. Improving situational awareness should be a key priority against the background of a situation involving many different stakeholders with potentially conflicting interests.

- Measuring and identifying specific ICT security risk factors is complicated by the inherent uncertainty surrounding which actors are involved, their capabilities as well as their motivations. While the overall landscape is known, what is unknown is the relative likelihood of one risk over another and the direction in which the threat is likely to evolve. This leads to general lack of knowledge on a systemic level. This also aggravates the lack of knowledge on a strategic level as predictions inform policymakers and guide their strategies. However, oftentimes policymakers simply do not understand the technical and managerial specificities of cyber security. Many leading officials in defense and foreign affairs departments are trained in international affairs and so, in some ways, speak a different language than the technical cyber experts. This gets in the way of sound cyber security policy-making.

- The new reality presented in the expert and foresight literature of an increasingly decentralized and privatized cyber security landscape forces governments to think about how they can incentivize private actors – both companies and individuals – to take a larger share of responsibility for the inter(national) cyber security posture since they are also the major source of current threats. One way could be to make them financially liable for weaknesses that they introduce to cyberspace. Analogies to public health are useful where, for example, in the case of swine flu, sick individuals were not allowed to board airplanes and the state intervened because individuals could harm the common good. And like in public health, some countries will focus more on prevention (e.g. education on hygiene) whereas others will focus on emergency response capabilities to pandemics.

- Given that cyber security threats are not like traditional, territorial-based threats that take years or months to emerge or evolve, but instead sometimes take just hours, response times need to be dramatically reduced. In other words, cyber security demands that states be agile. This issue of agility arises between states and the private sector as well as with other states at an international level. Specifically, in light of rapidly evolving state of the art of information communication technology, this brings the issue to the fore as to the shape and content of an effective cyber arms control treaty.

- Societies should avoid separating the security dimensions of cyber from the non-security ones – we need an integrated approach in which all (dependent) dimensions are included. Societies should not allow the security community to over-securitize this topic but at the same time, neither should they allow others to neglect legitimate security issues.

- A key question for societies will be how to allocate responsibility for defense and security across different government departments and between government and the private sector. The answer to this question will necessarily encompass multiple dimensions. Solutions may be found in the organizational realm (such as implementing the principle of subsidiarity) as well as in the technological.

- For our defense organizations in particular the central issue at stake is what this will mean for the traditional services: does this cross-cut the existing structure? Does it require a new service (like the US Cyber Command for instance)? And if it does, how do our defense organizations determine balance of investment issues?

Above all, it is clear that adequately dealing with these issues way will be vital to ensuring the well being of our societies business continuity in the years to come.

APPENDIX I: BIBLIOGRAPHY OF FORESIGHT REPORTS

Anderson, J.Q. and Rainie, R. *The Future of the Internet II* (Washington: Pew Internet, 2006). http://www.pewinternet.org/~/media//Files/Reports/2006/PIP_Future_of_Internet_2006.pdf.pdf.

---, *The Future of the Internet II* (Washington: Pew Internet, 2006). http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_FutureInternet3.pdf.pdf.

Andrews, K., Crawhall, R., Smith, J., and Spring, L. *Global Security Scan for Canadian Science Capabilities (2015 – 2020): Report of Proceedings* (Shirley's Bay: Centre for Security Science, 2008). http://cradpdf.drdc.gc.ca/PDFS/unc84/p531488.pdf.

Auger, J. and Wimbish, W. eds. *Proteus Futures Digest* (Carlisle Barracks: Proteus, 2007). http://www.carlisle.army.mil/proteus/docs/auger-proteus-futures-digest-2007.pdf.

Ayers, C.E. Cetron, M.J., Davies, O., and Steele, S.F. 'World War 3.0: Ten Critical Trends for Cybersecurity.' *The Futurist* 43:5 (2009). http://www.allbusiness.com/government/government-bodies-offices/12858412-1.html.

Bellovin, S.M., Benzel, T.V., Blakely, B., Denning, D.E., Diffie, W., Epstein, J., and Verissimo, P. *Information Assurance Technology Forecast 2008* (Washington: IIEE Computer Society, 2008 http://cmuportugal.di.fc.ul.pt/docs/InfoAssuTechForecast-ieee-Sec&Priv-jan08.pdf.

Bivins R.L.,Condray, P.M., Fecteau, M.D., and Smith, K.C. *Alternate Futures for 2025: Security Planning to Avoid Surprise* (Washington: Air Force 2025, 1996).
http://csat.au.af.mil/2025/a_f.pdf.

Cetron, M.J. *55 Trends for Cyberwar* (Newton: Forecasting International,2009).
http://www.davidleffler.com/55-Trends-for-Cyberwar.html#_Toc224031539.

Chupa, J. and Schneider, S. *Innovation Trends in Cyber Security* (London: Global Security Challenge, 2009). http://globalsecuritychallenge.com/Innovation%20Trends%20in%20Cyber%20Security.pdf.

Colarik, A. and Janczewski, L. Eds. *Cyber Warfare and Cyber Terrorism* (Hershey: IGI Global, 2007).
http://www.igi-global.com/downloads/excerpts/reference/IGR4726_WbOBBAVgQ2.pdf.

Conetta, C.. *Arms Control in an Age of Strategic and Military Revolution* (Cambridge: Project on Defense Alternatives, 2005).
http://www.comw.org/pda/0511rm11.html.

Convertino II, S.M., DeMattei, L.A., and Knierim, T. M. *Flying and Fighting in Cyberspace* (Maxwell AFB: Air University Press, 2007).
http://www.au.af.mil/au/awc/awcgate/awc-mxwl.htm.

Copeland, T.E. (ed.), *The Information Revolution and National Security* (Carlisle Barracks: Strategic Studies Institute, 2000). http://www.strategicstudiesinstitute.army.mil/pdffiles/pub225.pdf.

Curtis, N. J. and Dortmans, P.J. *Towards an Analytical Framework for Evaluating the Impact of Technology on Future Contexts* (Edinburgh: DSTO Systems Sciences Laboratory, 2004).

Decker, A. *The Future of Cybercrime – Challenges and Solutions*, (Council of Europe Panel Discussion), 2009. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20interface%20

2009/if_2009_presentations/A_Decker_CoE-The_future_cybercrime_Challenges_Solutions.pdf.

Denning, D.E. 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy.' In Arquilla, J. And Ronfeldt, D. *The Future of Terror, Crime, and Militancy* (Santa Monica: RAND Corporation, 2001). http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf.

Devine, J. 'Tomorrow's Spygames,' *World Policy Journal* 25, no. 3 (2008): 141-151.

Dickson, S.A. *Enabling Battlespace Persistent Surveillance: The Form, Function, and Future of Smart Dust* (Maxwell AFB: Air War College, 2007). http://www.au.af.mil/au/awc/awcgate/cst/bh_dickson.pdf

Dombrowski, P. *Alternative Futures in War and Conflict: Implications for U.S. National Security in the Next Century* (Newport: Naval War College, 2000). http://www.au.af.mil/au/awc/awcgate/navy/alt_futures.htm.

Ghosh, S. 'The Nature of Cyber-attacks in the Future: A Position Paper.' *Information Systems Security* March / April 2004: 18-33. http://www.auerbach-publications.com/dynamic_data/3093_1854_cyberattacks.pdf.

Klaver, M.H.A., Luiijf, H.A.M. 'Cyberspace als militaire dimensie', TNO DV 2010 A136, July 2010.

Kuehl, D.T. and Miller, R.A. 'Cyberspace and the 'First Battle' in 21st-century War,' *Defense Horizons* no. 68 (September 2009). http://www.ndu.edu/press/dh/DH68.pdf.

Larsen, A. And Smith, J.M. *All Our Tomorrows: A Long-Range Forecast of Global Trends Affecting Arms Control Technology* (USAF Academy: USAF Institute for National security Studies, 2002). http://www.usafa.edu/df/inss/OCP/OCP44.pdf.

Lippis III, N.J.. *Global IT Security Threat Trends and Future Outlook* (Hingham: Lippis Report, 2009). http://www.ciscosystems.md/en/US/solutions/collateral/ns340/ns394/ns171/ns441/LippisRpt_130.pdf.

Luker, J.J. *State Actor Threats in 2025* (Maxwell AFB: Air War College, 2007). http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA497566&Location=U2&doc=GetTRDoc.pdf.

Mazanec, B.M. 'The Art of (Cyber) War.' *The Journal of International Security Affairs* Spring, no. 16 (2009). http://www.securityaffairs.org/issues/2009/16/mazanec.php.

McAfee Avert Labs. 'The Future of Security,' *Sage* 1:2 (April 2007). http://www.mcafee.com/us/local_content/misc/sage_0407.pdf.

McAfee, Inc. *Virtual Criminology Report. Cybercrime: The Next Wave* (Santa Clara, 2007). http://www.mcafee.com/us/local_content/reports/mcafee_criminology_report2007_en.pdf.

McConnell, M. 'Cyberwar Is the New Atomic Age,' New Perspectives Quarterly 26:3 (2009). http://www.digitalnpq.org/archive/2009_summer/20_mcconnell.html.

Melikishvili, A. 'Recent Events Suggest Cyber Warfare Can Become New Threat,' *WMD Insights* no. 29 (December 2008/January 2009). http://www.wmdinsights.com/I29/I29_G3_RecentEvents.htm.

---. Mapping the Global Future (Washington, 2004). http://www.foia.cia.gov/2020/2020.pdf.

---. *NIC Speeches - The National Security Telecommunications and Information Systems Security Committee* (Washington, 2001). http://www.dni.gov/nic/speeches_telecommunications.html.

O'Hara, T.F. *Cyber Warfare/Cyber Terrorism: USAWC Research Project* (Carlisle Barracks, 1996). http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA424310&Location=U2&doc=GetTRDoc.pdf.

Office of the United States Director of National Intelligence. *Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence* (Washington, 2010). http://www.dni.gov/testimonies/20100202_testimony.pdf.

Paller, A. *Predicting the Future of Cybercrime and Security* (Bethesda: SANS Institute, 2007). http://www.bcs.org/server.php?show=ConWebDoc.8126.

Schafer, J.A. (ed.), *Policing 2020: Exploring the Future of Crime, Communities, and Policing* (Futures Working Group, 2007). http://www.policefuturists.org/pdf/Policing2020.pdf.

Stein, G.W.. *Information Attack: Information Warfare In 2025* (Maxwell AFB: Air Force 2025, 1996). http://csat.au.af.mil/2025/volume3/vol3ch03.pdf.

Stephenson, S.A. *U.S. Space Command's Role in Computer Network Defense: 2020*
Vision or Hack Job? (Newport: Naval War College, 2002). http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA405816&Location=U2&doc=GetTRDoc.pdf.

Sund, C. 'Towards an International Road-map for Cybersecurity.' *Online Information Review* 31: (2007): 566-582.

Tangredi, S.J. *All Possible Wars?: Toward a Consensus View of the Future Security Enviroment, 2001-2025* (Washington: National Defense University, 2000). http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA421945&Location=U2&doc=GetTRDoc.pdf.

United States Department of Defense. *Quadrennial Defense Report* (Washington: Department of Defense, 2010). http://www.defense.gov/qdr/QDR%20as%20of%2026JAN10%200700.pdf.

United States Government Advisory Board Executive Writers Bureau. *Cyberterrorism: A look into the future* (2009).

http://www.infosecurity-magazine.com/view/5217/cyberterrorism-a-look-into-the-future/.

United States National Intelligence Council. *Global Trends 2015: A Dialogue About the Future With Nongovernment Experts* (Washington: National Foreign Intelligence Board, 2000). http://www.dni.gov/nic/PDF_GIF_global/globaltrend2015.pdf.

United States National Intelligence Council. *Global Trends 2025: A Transformed World* (Washington: National Intelligence Council, 2008). http://www.dni.gov/nic/PDF_2025/2025_Global_Trends_Final_Report.pdf.

APPENDIX II: ENDNOTES

1 Klaver, M.H.A., Luiijf, H.A.M., Cyberspace als militaire dimensie, TNO DV 2010 A136, juli 2010.

2 Only online, publicly-available foresight reports were analyzed; this study excludes other publications or media (such as blogs, magazines, and websites).

3 Based on data from http://www.ic3.gov/default.aspx.

4 Governments have issued various trend reports (for example, the CSI/FBI Computer Crime and Security Survey follow trends in this domain).However, we have not considered these as foresight studies.

5 Internet World Stats, *Internet Usage Statistics; The Internet Big Picture. World Internet Users and Population Stats*, 2009 <http://www.internetworldstats.com/stats.htm> [accessed 20 July 2010].

6 R. L. Bivins et al. *Alternate Futures for 2025: Security Planning to Avoid Surprise* (Washington: Air Force 2025, 1996): 60.

7 N. J. Lippis III. *Global IT Security Threat Trends and Future Outlook* (Hingham: Lippis Report, 2009).

8 S. M. Bellovin et al. *Information Assurance Technology Forecast 2008* (Washington: IIEE Computer Society, 2008) : 77.

9 C. Conetta. *Arms Control in an Age of Strategic and Military Revolution* (Cambridge: Project on Defense Alternatives, 2005): 14.

10 Based on Symantec Corp. Data. See http://www.symantec.com/business/theme.jsp?themeid=windows_datacenter.

11 Network convergence is the merging of data technologies 'to a point where all communications [...] are transported over a common network structure.' United States Office of the Director of National Intelligence. *Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on*

Intelligence (Washington, 2010), 3.

12 United States Office of the Director of National Intelligence. *Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence,* 4.

13 J. Devine. 'Tomorrow's Spygames,' *World Policy Journal* 25, no. 3 (2008): 141-151.

14 Joseph A. Schafer, ed. *Policing 2020: Exploring the Future of Crime, Communities, and Policing* (Futures Working Group, 2007): 209-210.

15 J. Chupa and S. Schneider *'Innovation Trends in Cyber Security* (London: Global Security Challenge, 2009): 5.

16 National Intelligence Council. *Mapping the Global Future* (Washington, 2004): 75.

17 The nature of future 'attacking actors' is discussed 49 times in our dataset, against only 28 times for cyberspace governance, the next-most-discussed issue.

18 Joseph A. Schafer, ed. *Policing 2020: Exploring the Future of Crime, Communities, and Policing*, 33.

19 S. M. Bellovin et al. *Information Assurance Technology Forecast 2008*, 77.

20 A. Melikishvili, 'Recent Events Suggest Cyber Warfare Can Become New Threat,' *WMD Insights* no. 29 (December 2008/January 2009): 25.

21 S. M. Bellovin et al. *Information Assurance Technology Forecast 2008*, 77.

22 R. A. Miller and D. T. Kuehl. 'Cyberspace and the 'First Battle' in 21st-century War,' *Defense Horizons* no. 68 (September 2009): 5.

23 R. A. Miller and D. T. Kuehl. 'Cyberspace and the 'First Battle' in 21st-century War,' 5.

24 T. E. Copeland, ed. *The Information Revolution and National Security* (Carlisle Barracks: Strategic Studies Institute, 2000): 91.

25 S. M. Bellovin et al. *Information Assurance Technology Forecast 2008*, 74.

26 Alice Decker. *The Future of Cybercrime – Challenges and Solutions*, (Council of Europe Panel Discussion): 2009.

27 C. Conetta. *Arms Control in an Age of Strategic and Military Revolution*, 11.

28 United States Office of the Director of National Intelligence. *Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence*, 3.

29 R. L. Bivins et al. *Alternate Futures for 2025: Security Planning to Avoid Surprise*, 60

30 Joseph A. Schafer, ed. *Policing 2020: Exploring the Future of Crime, Communities, and Policing*, 47.

31 Source: ITU World Telecommunication/ICT Indicators database. http://www.itu.int/ITU-D/ict/publications/world/world.html

32 N. J. Lippis III. *Global IT Security Threat Trends and Future Outlook*, 3.

33 National Intelligence Council. *NIC Speeches - The National Security Telecommunications and Information Systems Security Committee* (Washington, 2001).

34 McAfee, Inc. *Virtual Criminology Report. Cybercrime: The Next Wave* (Santa Clara, 2007): 7.

35 C. Conetta. *Arms Control in an Age of Strategic and Military Revolution*, 5.

36 McAfee, Inc. *Virtual Criminology Report. Cybercrime: The Next Wave*, 7.

37 C. Conetta. *Arms Control in an Age of Strategic and Military Revolution*, 19.

38 C. Conetta. *Arms Control in an Age of Strategic and Military Revolution*, 4.

39 C. Conetta. *Arms Control in an Age of Strategic and Military Revolution*, 14.

40 R. A. Miller and D. T. Kuehl. 'Cyberspace and the 'First Battle' in 21st-century War,' 6.

41 Aksel Ethembabaoglu et al., ICT-kwetsbaarheid en Nationale Veiligheid, Notitie No 02 | 10 | 10.

HCSS, LANGE VOORHOUT 16, 2514 EE THE HAGUE
T: +31 (0)70-3184840 E: INFO@HCSS.NL
W: STRATEGYANDCHANGE.NL