EastWest Institute

Resetting the System

Why highly secure computing should be the priority of cybersecurity policies

DISCUSSION PAPER

1/2014

Resetting the System

Why highly secure computing should be the priority of cybersecurity policies

By **Sandro Gaycken** & **Greg Austin**

January 2014

shift
enter
delete

About the Authors

Dr. Sandro Gaycken is a senior researcher in computer science at the Free Univeristy of Berlin, with a focus on cyber war. He is a senior fellow at the EastWest Institute, a fellow of Oxford University's Martin School, a director in NATO's SPS program on cyber defense, and he has served as a strategist to the German Foreign Ministry on international policy for cybersecurity in 2012-2013.

Dr. Greg Austin, based in London, is a professorial fellow at the EastWest Institute and a visiting senior fellow in the Department of War Studies at King's College London.

The authors would like to thank Felix FX Lindner (Recurity Labs Berlin), John Mallery (MIT), Neil Fisher (Unisys), Doug Mackie (Georgia Tech), Kamlesh Bajaj (DSCI), and, from EWI, John Mroz, Bruce McConnell, Karl Rauscher, James Creighton, Andrew Nagorski, Sarah Stern and Franz-Stefan Gady, for a critical review and their helpful comments.

The EastWest Institute seeks to make the world a safer place by addressing the seemingly intractable problems that threaten regional and global stability. Founded in 1980, EWI is an international, non-partisan organization with offices in New York, Brussels, Moscow and Washington. EWI's track record has made it a global go-to place for building trust, influencing policies and delivering solutions.

The EastWest Institute
11 East 26th Street, 20th Floor
New York, NY 10010 U.S.A.
+1-212-824-4100

communications@ewi.info
www.ewi.info

EXECUTIVE SUMMARY

As state-sponsored intrusions and high-end criminal activity in cyberspace have evolved, they are producing novel kinds of risks. Our present security paradigms fail to protect us from those risks. These paradigms have tolerated inherent structural security deficits of information technology for too long; they create the impression that policy is simply captive to this highly vulnerable environment. A new remedy favored in some countries seems to be active defense, but this emerging preference may be ineffective and more dangerous than helpful.

We call for a new ecology of cybersecurity. It is based firmly on the disruptive concept of highly secure computing, relying primarily on passive security measures, independent of attack attribution. It also helps to preserve freedom and privacy. Our approach is based on a reassessment of the balance between four components of cybersecurity: the public needs in the face of novel and serious risks; the relative security levels of commercially available technology; disruptive options for high security technologies; and patterns of policy and market behavior in the ICT sector. It will recommend strategic government intervention to overcome persistent market and policy failures and to stimulate wider investment in and application of the necessary technologies.

Due to its growing urgency and in light of its alternatives, we propose highly secure computing as a new priority for cybersecurity policies internationally. Governments should send clear signals to enable security-driven IT innovation, starting top-down with the highest security requirements in the highest value targets. They should cooperate internationally to realize this new paradigm quickly and to stem the evolution of high-end cyber attackers before they can inflict more damage. Once adopted, this new paradigm would help the market to adjust by itself and open up interesting new lines of commercial opportunity, thus becoming a win-win-win strategy for security, freedom and prosperity.

Introduction

International peace and economic stability depend ever more greatly on critical information infrastructures. Unsurprisingly, increasingly sophisticated attackers emerge, willing to exploit these dependencies. Yet at the same time, security is not growing more mature. Most of the security industry and research still focus strongly on the cybersecurity problems and tactics of the 1990s—hit-and-run, end-user-oriented computer fraud, hacktivists' website defacements, denials of service, and similar petty cyber crimes and low tech intrusions. The challenges presented by a permanently altered, novel security environment with an entirely new set of requirements are largely unappreciated. As a result, insecurity and cyber risks are rising significantly.

For a long time now, the dominant approach to cybersecurity has been based on the public health model in which education, monitoring, epidemiology, immunization and incident response were the key planks.

As the technical chapter of the International Telecommunication Unit (ITU) High Level Experts' Group report said in 2008: "Today's computing environment is global, with data flows traversing many geographies, and users accessing networks and application from virtually anywhere. Security requirements vary widely in different segments of global computing environments, ranging from acceptable (but not impregnable) to environments where security is frequently overlooked." Even the assumed high security in a handful of sectors in a few advanced economies (such as civil nuclear power or financial services in the United States or Europe) is now in question, with U.S. security agencies reporting rising concern about the possible vulnerabilities of information systems that were previously understood to be high security. Those concerns even extend to the military and intelligence domains.

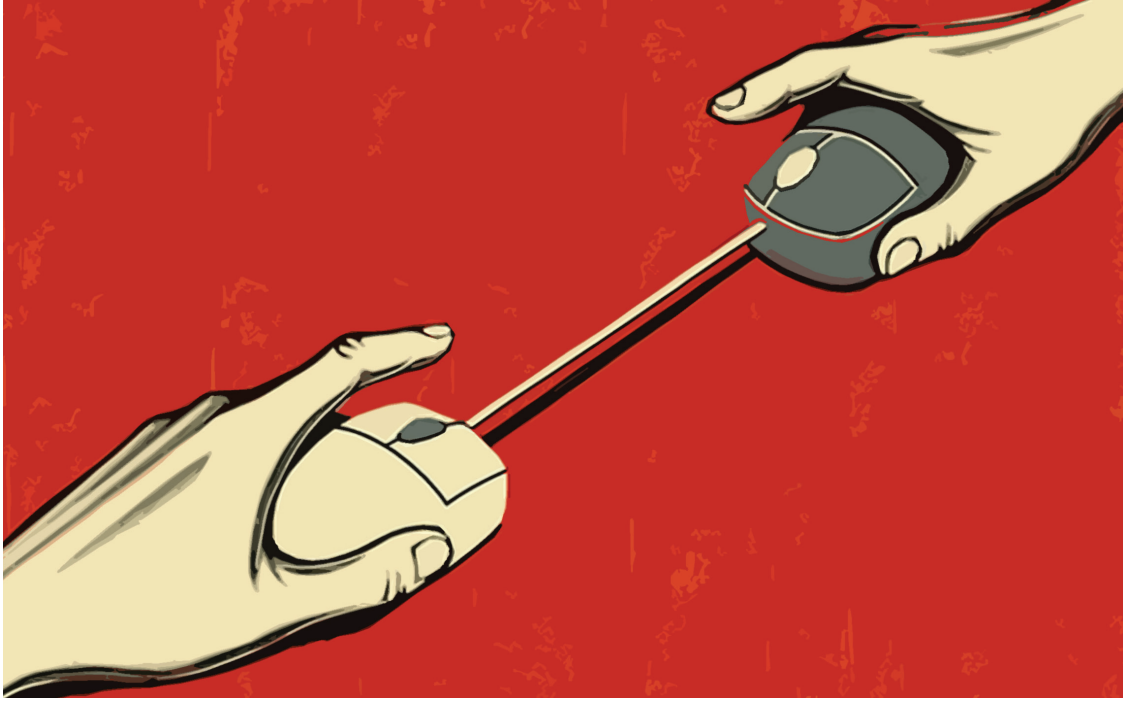
State actors have emerged as the greatest potential threat to critical information infrastructures on which international peace and economic security depend.[1] They can undertake sabotage and espionage in many segments of any digital society, producing different kinds of strategic damage while being almost invisible. They pose a huge challenge, one that should be tackled urgently. In addition, societies also need to develop more effective cyber defenses against larger criminal organizations and terrorist groups—as well as against a handful of irresponsible states.

For a long time now, the dominant approach to cybersecurity has been based on the public health model in which education, monitoring, epidemiology, immunization and incident response[2] were the key planks. This model did not provide sufficient security, not even against petty criminals. It may now be time to devote far greater attention to the creation of healthier, more resilient systems with inherent immunity even against high-end attackers.

In fact, we face such a rapidly changing threat that leading actors now prefer a military model to a public health model. To compensate for the lack of technical protection, many states and corporations are looking at active defense ("hack back & deter"). But this ap-

1 In this article, the authors want to follow the advice of Brookings' Allan Friedman who suggested "caution against conflating different threats simply because they all involve information technology. He added: "Crime, espionage and international conflict are very different threats, and grouping them together can lead to poorly framed solutions." The authors are interested in addressing nationally significant cyber threats, such as cyber warfare and cyber espionage, while noting that many of the solutions in this domain might have relevance to lower level threats at an enterprise or personal level. See Allan Friedman, "Economic and Policy Frameworks for Cybersecurity Risks," Center for Technology Innovation, Brookings Institution, 2011, p. 1. Friedman advocated the need to disambiguate cybersecurity as a multi-level problem by focusing on an "economic approach": "The economic approach to information security focuses on the incentives of these actors, and whether these incentives align with a socially optimal level of security" (p.5). We very much agree with this approach.

2 The EastWest Institute, "The Internet Health Model for Cybersecurity." 2012, http://issuu.com/ewipublications/docs/internethealth?e=1954584/2708658



proach is beset with problems.[3] It is politically fraught, and is viewed negatively in countries where public opinion is opposed to the massive surveillance capability that goes with it. Moreover, it is strategically destabilizing, as it invites escalation. And its effectiveness is reduced whenever attribution is not fully clear.

A different, more solid paradigm would be highly desirable. It would depart from traditional IT security and acknowledge the existence of very powerful new attackers, while bolstering online privacy and Internet freedom and avoiding the problems of attribution. To create such an approach, the concept of highly secure computing has to become a focus of renewed scientific research, industrial design and public policy.

The authors are aware that "highly secure computing" is not a widely used term.[4] We understand it to mean "information technology with high security," with "highly secure" implying "likely to be breached only in exceptional and rare circumstances and at high costs and risk." We agree with John Dobson and Brian Randell, who were critical of those who believed it possible to "construct totally secure computing systems."[5] But, significantly, these two scholars are also among those who have held up highly secure computing as a worthwhile goal for scientific research and public policy.

This EWI discussion paper also takes some inspiration from the joint IEEE-EWI report of 2010 on the *Reliability of Global Communications Cable Infrastructure*, which was the product of multi-sector consultations and which called for new measures to ensure highly reliable, robust and secure international communications infrastructure.[6]

This paper will: (1) comment briefly on the systemic information security threats from states as an enduring and dominating reality; (2) argue why active defense is more dangerous than helpful; (3) propose a different paradigm, that of highly secure computing, which matches the actual threat; (4) discuss why this paradigm has not been prominent in the past; (5) detail suggestions for possible response; and (6) review the international or diplomatic dimension.

The concept of highly secure computing has to become a focus of renewed scientific research, industrial design and public policy.

3 See Jody Westby, "Caution: Active Response to Cyber Attacks Has High Risk," Forbes.com, November 29, 2012, www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/.

4 Another, more common term could be "trustworthy computing," but this notion doesn't focus on the high end of a computer's inherent security. Also, note that much of our proposed approach is not about the Internet. Securing the endpoints, the hosts of the networks, is more important and more effective than securing the paths leading there.

5 J. E. Dobson and B. Randell, "Building reliable secure computing systems out of unreliable insecure components," IEEE, first published in 1986, republished in the Proceedings of the 17th Annual Computer Security Applications Conference, 2001.

6 IEEE and the EastWest Institute, "Reliability of Global Undersea Cables Communications Infrastructure," 2010, http://www.ieee-rogucci.org/files/The%20ROGUCCI%20Report.pdf.

The Threat Trend: Cyber War May Take Place

Cyber warfare is already judged to be strategically valuable, and even essential by at least 10 countries. Once it has been professionalized and further commodified, its efficiency will be multiplied and it will become a golden tool for many.

As mentioned above, state actors and their strategic cyber operations should be the main security concern of those seeking international collaboration in cyberspace. Organized crime and terrorists will also remain among the high-grade threats as their capabilities continue to shift toward systemic threats with the potential to disrupt national security, economic prosperity or social stability on a larger scale. The activities that pose national-level security threats are currently undergoing two kinds of evolution.

The first kind of evolution is conceptual. It is concerned with strategic ideas and doctrines. Signals intelligence (intercept and decoding of secret communications) and electronic warfare (disrupting and altering signals and data on the battlefield) were the principal applications of offensive national cyber capability until 15 years ago. But now it is clear to most strategists and tacticians alike that cyber operations can do much more. They are a golden key to any kind of digital society—a multi-purpose tool to manipulate it, a magnifying glass to observe it and a hammer to disrupt it.

One new avenue of strategic thought is concerned with deterrence doctrine, which allowed for a favorable military balance of power. It is currently undergoing a transformation in a number of ways under the influence of a spectrum of emerging offensive cyber-attack capabilities. A "targeted capability" can demonstrate mastery to attack only systems used for specific military, economic or political purposes. A "general capability" can demonstrate mastery to attack any kind of system, posing a broader threat, with an ability of "assured disruption" of the vital IT services and data highways. The ability to create a "forced transparency" can lead to the collection of secret information. Many other such postures for deterrence are conceivable.[7]

Other kinds of novel strategic thinking are concerned with the higher-order consequences of military or intelligence cyber-operations, with an optimization of the exploitation of results or with novel kinds of strategic cyber-operations. Such operations might aim to manipulate the digital flow of facts and opinions (information operations). Or they could weaken an adversary's economic and geostrategic power through economic espionage and sabotage or financial manipulation. All of this is possible and, if executed properly, could produce the desired strategic outcome at reasonable cost.

The second kind of evolution is operational. This level is concerned with techniques and tactics below the strategic level. Here there is considerable room to believe that past incidents might not be strong indicators of the efficiency of future cyber operations. They were bulky, complicated and expensive, with uncertain outcomes and a limited understanding of long-term collateral damages.[8] Their cost relative to gain had been seen as so questionable that it has prompted authors like Thomas Rid and Peter McBurney to argue that cyber warfare will be too expensive and attacks too monolithic to ever form a solid new paradigm.[9]

But these scholars may have looked more at an isolated piece of recent history, mistaking it to be state-of-the-art rather than a prototype. Assuming this latter view, military cyber attacks may yet be a new paradigm in IT, merely nascent and not yet in some final stage. Hacking in the service of state security, broadly defined, is just another IT market. It consists of programming software (known as "exploits") and of constructing hardware (such as an infected supply chain) for a specific and in this case novel and demanding purpose (defeating target security systems). Viewed as such, military hacking is presently in its infant, "backyard garage" stage of market-readiness, which may yet be developed

7 See: S. Gaycken, "Cyber as Deterrent" in: Maurizio Martellini (ed.), Cyber Security: Deterrence and IT Protection for Critical Infrastructures, Springer Briefs in Computer Security, December 2013.

8 Regarding the aspect of collateral damages, see Austin, The Costs of American Cyber Superiority, (http://ewipolicy.tumblr.com/post/57507054358/costs-of-american-cyber-superiority) and Gaycken,"Stuxnet and Prism – Symptoms of a Policy Failure," *International Politics Journal*, July 2013. Online at: https://ip-journal.dgap.org/en/ip-journal/topics/stuxnet-and-prism-symptoms-policy-failure.

9 Thomas Rid & Peter McBurney (2012): Cyber-Weapons, *The RUSI Journal*, 157:1, 6-13.

into a mature, "megacorp" stage.[10]

There are in fact many indicators for this development, and they already sketch a scary picture for our future cybersecurity. In the past five to 10 years, hacking has experienced the most well-funded and systematic development in its history in some 15 countries. We know more about this in the case of the United States because it is an open society. As stated in a 2012 Top Secret U.S. Presidential Directive on cyber operations, its goal is to develop "unique and unconventional capabilities to advance national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging."

This systematic development of hacking involves a number of steps. Methods from commercial, team-oriented, agile software development are applied to the illicit exploit-development process, producing highly flexible and adaptable, reusable modularized attacks, tools and toolsets. A systematic view of attacks is being developed, covering not only the aspect of penetration, but a whole attack cycle,[11] with the development of specific technologies and expertise at every step. Attacks are conceptualized as a software system (like a standing warfare unit that can deployed over and over again), and are not confined to just a single specific one-off event. The attack system can fulfill many functions simultaneously and threaten many different layers of the target—among those most notably the technical and organizational safety and security environment. These methods are fused with methods from the old days, from professional intelligence collection and systematic sabotage.[12] And the supporting ecosystem is being generated as well. A cyber-military market is presently evolving, with interesting fusions of small hacker firms, traditional IT corporations and defense industry enterprises. These actors are looking to take advantage of legal loopholes or create legal innovations for cyber attack and are adapting their organizational structures accordingly.

If this operational evolution in state hacking is taken into account and its strategic value acknowledged, there is evidence of the feasibility and efficiency of cyber warfare. Cyber warfare is already judged to be strategically valuable, and even essential by at least 10 countries. Once it has been professionalized and further commodified, its efficiency will be multiplied and it will become a golden tool for many.

Active Defense: Political Character and Operational Risks

How can this new kind of hacker, the state-sponsored cyber attacker, be confronted? Traditional IT security and its social management are clearly not up to this task. Leading governments, corporations, computer scientists and civil society leaders have said so repeatedly. Current policies are mostly *ad hoc* or *ex post facto* (detection-focused and reactive) and overly accepting of a highly vulnerable IT environment, where few of the existing vulnerabilities and vectors can be secured in advance. These security paradigms do only a mediocre job against teenagers and petty criminals and provide no serious defense against highly organized, well-resourced attackers.

There is some proof of this hypothesis. According to material leaked by Edward Snowden, the U.S. conducted 231 offensive cyberoperations in 2011, while simultaneously investing $652 million to plant thou-

How can this new kind of hacker, the state-sponsored cyber attacker, be confronted? Traditional IT security and its social management are clearly not up to this task.

10 The concept of megacorporation is a term of modern political discourse meaning a corporation that rivals the power of a state with sufficient power to act independently of the law or social norms.

11 Involving concepts and procedures from reconnaissance and footprinting, acquisition, development, testing and field-testing, to infiltration and penetration, escalation of privileges, exploit maintenance, deception, discovery-evasion, information extraction or sabotage, to exfiltration, deletion or planting of traces, and quality assurance.

12 Including "venus traps" or the very old kinetic means of security, as the recent shooting of the cybercommander of Iran suggests. See: http://www.telegraph.co.uk/news/worldnews/middleeast/iran/10350285/Iranian-cyber-warfare-commander-shot-dead-in-suspected-assassination.html, accessed November 18, 2013.

sands of backdoors in our IT-ecosystem.[13] Given the NSA's budget and expertise, this sounds quite plausible. China, Russia and other countries are almost certainly undertaking similar activities. Yet only one of these operations has been detected to date (the espionage operation dubbed "Flame ") and not a single backdoor has been found. Activities from other states are equally invisible. This clearly points out the severe incapacities of passive defense based on commercially available detection and monitoring techniques. Apart from an awful detection rate, detection times are equally disturbing. In the few cases which have been detected, the first detection took place several months, or more commonly, several years after the initial infection, and it was mostly by happenstance or crude mistakes of the attacker, not by the sets of sensors and analyses.

Identifying nation-state attackers who care about camouflaging their cyber espionage and sabotage efforts is extremely difficult.

At the same time, militaries around the world, critical infrastructures, and the global and national economies are highly dependent on the underlying, highly vulnerable systems. This problem is well known to governmental cyber strategists. As a result, there is increased emphasis on active defense. If passive defense is not possible, the thinking goes, active defense has to compensate.

At the strategic level, the prevailing doctrine of active defense reflects an operational preference which can be characterized as "profiling and retaliation." Attackers are identified through a collection of forensic data traces at the scene of the attacks and in the networks. The goal is then to threaten and discourage or deter them. This approach entails surveillance on a scale and reach not fully revealed to the public, despite the recent cascade of leaks, and even a pre-emptive hacking of foreign IT environments for closer observation. While the countermeasures are aimed primarily at foreign adversaries, others—including allies—are also targeted. The recent furor in Germany and Brazil in reaction to the NSA programs revealed by Edward Snowden illustrates the kind of the backlash such measures can produce. There is global disquiet about widespread preemptive hacking of foreign networks simply to get better monitoring coverage not linked to specific threats; it is seen as an unacceptable assault on national sovereignty and citizens' privacy.

More fundamentally, the profiling and retaliation approach is not effective. It assumes that it is not so difficult to prove the identity of an attacker, and that attribution through profiling can be plausibly defended. The Mandiant report[14] of February 2013 focusing on China's economic espionage is an excellent example of this approach. The company profiled and identified Chinas APT-1 group, a military cyber espionage unit. But it also demonstrated the limits of its underlying techniques of analysis, as the identification wasn't very hard. A number of traces were quite obvious. The report rather supports the impression that the attackers did not seem to have cared about covering up their tracks. They only applied a very rudimentary set of disguising measures to begin with, although Chinese technical and military writing suggests that the country's cyber experts have a thorough knowledge of techniques for spoofing and hiding. The little care applied to camouflage seems an expression of strategic impunity—"What are you going to do about it anyway?" In conclusion, Mandiant's effort has not proven the effectiveness of profiling. It has only proven the effectiveness of profiling attackers who do not care about their traces.

Identifying nation-state attackers who care about camouflaging their cyber espionage and sabotage efforts is extremely difficult. They will never operate from home, and if they apply the full range of state-of-the-art techniques for deception and disguise, false indicators are always more numerous and convincing than the true ones. And this is just today's situation. Advanced techniques for evasion and deception will be an important part of the evolution of offensive weapons. The first signs of such a move toward more systematized deception can be seen in some current research. For example, one avenue of investigation applies artificial intelligence, big data analytics and machine learning algorithms to generate automated, systematic deception of profilers.

How does this work? The deceiver monitors

13 See: http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html, accessed November, 18 2013.

14 Mandiant Intelligence Center Report, "APT1: Exposing One of China's Cyber Espionage Units," 2013, intelreport.mandiant.com.

all activities of the profiler for a while by sitting as a hidden "middle man" between him and the attacker he is analyzing. After a while, the deceiver will know what the profiler is looking for, and he will know how typical adversaries of the profiler work. Then the deceiver takes over. He can attack the profiler's systems and leave fabricated deceiving traces the profiler could readily accept, emulating coding practices, even using entire sequences from the arsenal of the previous attacker. He can intercept the profiler's attempts to find out more and redirect those investigations onto automatically prepared false traces, which match the profiler's preconceptions about the presumed adversary. Most of that will be fully automated. Of course there might be some traces of the original attacker as well. But there is always some noise to be filtered out.

So will the "real" traces ever be found among the overwhelming evidence pointing to a more "natural" foe? Will the analyst see through the traps and understand them as the work of a master deceiver? Could the defender then have sufficient confidence to act politically or militarily against the deceiver? This uncertainty may become even more exaggerated with the advent of "big data profiling." Ever more data to analyze can lead to ever more confusion.

As long as digital traces are the main lead to an attacker, the goal of establishing attribution at the level of confidence necessary to justify official retaliation may be unreachable. U.S. intelligence sources have suggested repeatedly in private and in public that they do not rely exclusively on digital traces. Yet there are doubts about the availability of non-digital corroborating data from classical human intelligence. Offensive cyber units can be very small. A team of 15 to 20 attackers can already be very effective, if led by one or two "wizards."[15] And they can be hidden very well. Getting human insiders into all of these highly secret teams and activities will be close to impossible—especially since offensive cyber capabilities are not limited to just the most powerful nations. Sooner or later—if not already—there will be hundreds of such units around the world.

Some authors have argued that the problem of attribution is not relevant for cyber warfare, as the military attacker always wants to be identified: "The notion that a powerful state actor would try to coerce another actor anonymously is highly unrealistic."[16] But cyber is a novel kind of warfare. It can wreak havoc of more significant geostrategic impact through invisible, non-attributable manipulation, creating silent and secret erosions of an economy, of military technology, through false flag operations, or even through "anonymous and pseudonymous deterrence," hinting that any kind of activity might have cyber consequences. These cyber operations may be most effective *precisely* on those occasions when the attacker is not identifiable. Visible attacks could trigger instant retaliation, possibly including armed counterattacks, nullifying the attacker's activities from the outset.

Summing up, a security strategy based on active defense, and more narrowly, on profiling and retaliation is not a good idea, in fact even dangerous. Profiling is simply too uncertain, and it might lead to intended or unintended escalations, destabilizing international security at large.

A security strategy based on active defense, and more narrowly, on profiling and retaliation is not a good idea, in fact even dangerous.

The Alternative of Highly Secure Computing

Fortunately, we are not out of options. Why not get the basic technology secured so no one can attack strategically critical systems in devastating ways in the first place?

For decades, computer science has had a large array of unconventional ideas about how to reach very high (inherent, not reactive) security. Many of these ideas are already visible in a range of applications from secret research laboratories to new mainframe computer designs, and from the control of civil nuclear power facilities to command and control systems for planet-threatening nucle-

15 In IT-lingo, a wizard is someone who can code intuitively and so outstandingly well that what he does seems like magic to outsiders.

16 Thomas Rid, *Cyber War Will Not Take Place*, Hurst & Co, London, 2013, p. 159. Rid offers a nuanced evaluation of the attribution problem, conceding that "the attribution problem is almost never perfectly solved" (p. 156). Yet as argued above, the present authors would not agree with Rid's emphasis on espionage as the best example of cases where states would not want to be identified as the source of a cyber operation (p.158).

ar missile systems. If applied more widely, the high security computing technologies could solve a large part of the cybersecurity problem for good.

These ideas have just never been very prominent. In the past, the threats were not as serious as the ones we face today, which was why traditional IT security was deemed sufficient. Besides, most of these high security technologies have been associated with high costs and loss of easy functionality. But times have changed. Hacking has grown into a professional, serious threat, and our prevalent paradigms of IT security are failing us. The time is ripe for high-security IT. It has to leave the universities, the research centers and ministries of national defense and take root in the broader community. Below are several fundamental elements of "highly secure computing" and a brief discussion on why they were never implemented on a mass consumer basis:

Hacking has grown into a professional, serious threat, and our prevalent paradigms of IT security are failing us.

Architectural redesign: Architectural redesign of computers aims to enable the technology to distinguish between data (the information being manipulated) and programs. The present infrastructure is based predominantly on a "von Neumann" design, which doesn't provide this option. Consequently, attackers can abuse a computer mechanism causing it to read data that will make it execute a program differently, and thereby install an attack. This kind of architecture triumphed over the so-called "Harvard architecture" back in the mid-1940s. The latter was an alternative design which would have enforced the distinction between data and executables, rendering attacks much more difficult. But von Neumann architectures had less need of memory, so they were significantly cheaper and performed better at the time.[17] Over the past decades, varieties of novel architectural approaches have been proposed to move away from von Neumann and back towards a Harvard architecture. Thus far, however, they have only been implemented in a selection of "embedded systems"—computers, which are controlling parts of machines. Leading private sector firms, such as Intel and Texas Instruments, have used elements of Harvard architecture in some of their products, but not broadly. Other architectural ideas for high security are available as well, such as "moving target" architectures, which change some their configurations every now and then, making it harder for attackers to keep their attacks from malfunctioning.

All architectural measures can offer security on a very basic level, thus providing good security scaling effects throughout the system.

Data flows: It would also be possible to largely disable a flow of illegitimate activity from one area of an IT environment onto another, making it harder for an attacker to move inside a penetrated system. One such attempt consists of "separation and partition kernels." These are operating systems that are not able to execute different kinds of code in different functional segments of a computer. These kernels have been researched since the 1980s,[18] but, again, there are only a very few examples of implementation of this idea and these are in very specific niche markets.[19] Another approach, "information flow control," seeks to hinder the movement of an attacker and of stolen data inside a computer. This idea, dating back to the 1970s,[20] aims to tag and control the flow of information inside a computer or a smaller network of computers, by recognizing which data is trying to flow and disrupting unauthorized or illegitimate flows of data either for propagation or exfiltration. But information flow control is not frequently implemented. It consumes resources, delays the data streams (which is unacceptable to most users) and makes sharing more complicated, rendering this approach costly and unattractive.

Minimal complexity: Another set of ideas aims to reduce computational complexity—a distinct priority for efforts to enhance security. Microkernels are the most prominent idea in this strategic approach. These kernels are tiny operating systems consisting of much

17 Paul E. Ceruzzi. *A History of Modern Computing*, 2nd ed., MIT Press, Cambridge MA, 2003, pp. 21 and 23.

18 See John Rushby, "The Design and Verification of Secure Systems," Eighth ACM Symposium on Operating System Principles, pp. 12-21, Asilomar, CA, December 1981. (*ACM Operating Systems Review*, Vol. 15, No. 5).

19 One example is Green Hill's "Integrity-178B," a separation kernel used in aviation. See for technical specifications: http://www.niap-ccevs.org/st/st_vid10362-st.pdf.

20 Dorothy E. (& Peter) Denning. 1976. A lattice model of secure information flow. *Commun. ACM* 19, 5 (May 1976), 236-243.

less code than conventional operating systems. Microsoft's Windows 7 consists of an estimated 80 million lines of code and Apple OS X of a similar number; by comparison, an seL4 microkernel consists of just roughly 7,000 to 10,000 lines of code (SLOC can be understood in different ways and the estimates used here are meant only to illustrate orders of magnitude of difference.)

This difference is hugely important for the control and the transparency of the computer. A system with millions or tens of millions of lines of code may have as many as tens of thousands of exploitable programming errors in it, which cannot be discovered automatically[21] or removed,[22] and it creates a lot of noise, while a system with only 10,000 lines of code behaves in a more clear-cut, observable manner and can be checked rigorously for any kind of exploitable weakness. The latter technical option is available now. One seL4 microkernel has just recently become what computer scientists call "formally verified."[23] Such an assurance process is hardly imaginable for most current commercial software or operating systems. The verification of only these few lines of code in the verified microkernel took a large team of highly qualified experts several tedious months, costing about US$10 million, and the verification only holds as long as the system is not significantly altered.

Yet again, even though such operating systems are much more secure, they are rarely used. Some have found an application in aerospace, though mostly for safety reasons, not primarily for security. A less complex system is also less likely to crash due to some internal conflicts or overloads. But outside of safety-heavy environments, there is little tolerance for this idea. Producers fear a loss of functionality, and any transition from the existing monocultures of operating systems to a new kind is considered too costly.

Language: Another high-security idea comes from the "LangSec" movement.[24] This idea relies on finding security through application of the philosophy of language. Computers not only do things they are not supposed to do based on the many mistakes in their program code, but also because their input from humans or other computers on networks is a language of its own. Languages, natural and formal, have a meaning, and meaning produces misunderstandings. A good example is Voltaire's half-joking remark: "If a diplomat says 'yes,' he means 'maybe.' If a diplomat says 'maybe,' he means 'no.' If a diplomat says 'no,' he is not a diplomat." The underlying idea of this joke is that the same expression can mean different things on different occasions. The same applies to computer languages. Depending on the code context ("semantics") or on the practical context ("pragmatics"), a similar expression can do different things. Intentionally causing such a divergent interpretation is the basis for the majority of today's attacks on computer networks. The LangSec movement actively advocates practical means to reduce language complexity and expressiveness in computer communication, much like early diplomacy developed the concept of protocols in order to reduce the chance for culturally caused misinterpretation.

Reducing network dependency: Finally, another rather simple step to much tighter security consists of "disconnecting the networks." A non-networked or just lightly-networked computer (and information society) is much harder to attack than one which is connected to everything. And a lot of critical systems like power plants or production facilities do not really have to be accessible through large external networks—be those

A system with millions or tens of millions of lines of code may have as many as tens of thousands of exploitable programming errors in it.

21 As all current computers are Turing machines, Rice's theorem applies. See: http://kilby.stanford.edu/~rvg/154/handouts/Rice.html, accessed 30th November 2013.

22 Removing a single vulnerability can cost up to $400,000. Removing tens of thousands will likely ruin companies – a reason why liability for programming errors has never been introduced. See also: Sandro Gaycken & Lindner, FX, "Zero Day Governance – An (Inexpensive Solution tot he Cyber-security Problem," University of Toronto, Harvard/MIT Cyber Dialogue 2012 Stewardship Papers, online at: http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012papers/CyberDialogue2012_gaycken-lindner.pdf, accessed 30th November 2013.

23 Klein, G., Elphinstone, K., Heiser, G., Andronick, J., Cock, D., Derrin, P., ... & Winwood, S. (2009, October). seL4: Formal verification of an OS kernel. In *Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles* (pp. 207-220). ACM.

24 See http://langsec.org/.

military networks like the U.S.-GIG[25] or the Internet. Upon critical review, in some cases, the net value of the "progressivist" impulse to network everything and everyone may be close to zero or even negative.

Thus, "we have the technology" for highly secure computing. Much of it has been available for a long time. It will not provide 100 percent security. This is not the goal. But a more aggressive take up of these ideas could help us do a lot better than we have been doing in information and systems security so far.

Getting the technology right for highly secure computing is quite possible. And it is desired.

This much higher level of basic security in software, OSs and hardware would render a lot of malicious hacking activity extremely expensive and carry more risk of discovery, discouraging most actors and activities. The problem of economic cyber espionage, for instance, is one that could be controlled by a set of high security computing measures. And what is even better about a high security IT approach is that it leaves much less room for pressure, in the name of political security, on existing standards of liberty and privacy. Highly secure computing is a concept of "deterrence by denial," crafted to render attribution strategically irrelevant. There will automatically be less use for active defense and much less need for surveillance and Internet control. Thus, highly secure computing is a win-win strategy for security and civil liberties.

In summary, getting the technology right for highly secure computing is quite possible. And it is desired. Look at the United States. The Department of Homeland Security declared in 2009 that scalable secure computing should be the first of 11 national priorities for research and commercial development against the background of the need to "transform the cyber-infrastructure so that critical national interests are protected from catastrophic damage and our society can confidently adopt new technological advances."[26] The DHS pointed out that "many gaps remain in reusable requirements for trustworthiness, system architectures, software engineering practices, sound programming languages that avoid many of the characteristic flaws, and analysis tools that scale up to entire systems. Thoroughly worked examples of trustworthy systems are needed that can clearly demonstrate that well-conceived composability can enhance both trustworthiness and scalability."[27] It argued that "formally inspired approaches may be more promising than any of the less formal approaches attempted to date." It admitted that building new scalable secure systems from the ground up may seem like a Herculean task, but then went on to say that it would be even harder to build such a system on the foundations of the vulnerable systems we have today.

Market Pressures and Policy Failures

So why isn't this done? If all of this has been well known for decades, why is highly secure computing rarely proposed as a priority goal? Why isn't it the focus of more attention in major policy statements, such as the United States' International Strategy in Cyberspace of 2011? In a few words, the necessary changes are expensive, and the choices lie largely in the traditionally free and largely unregulated market.

The persistence of insecurity we are seeing globally is caused by a combination of market pressures and policy failures in critical areas.[28] This is the essence of cyber insecurity, and it is not technical. Business consumers do not yet see the value of high security IT despite the heightened corporate risks and new international tensions. Many changes such as a move from von Neumann to Harvard architectures, or the shift from commercial operating systems to microkernels, are deeply architectural and would require an entirely new kind of computer. As the DHS research plan mentioned above, the more highly technologies could not be bolted on top of the existing ones. Much of the auxiliary equipment would have to be redesigned, too. Other changes such as disconnecting networks and controlling data streams could affect performance. So by and large, this kind of IT would require a gigantic initial investment, and it would be more expensive to operate in some respects,

25 GIG is the U.S.-military network "Global Information Grid."

26 Department of Homeland Security (DHS), "A Roadmap for Cybersecurity Research," 2009, p. Vii.

27 Ibid., 4.

28 For a more detailed analysis of the question of market failures in cybersecurity, see Friedman op. cit.

less convenient and less functional.[29] So consumers—firms and individuals—will not rush to adopt it voluntarily. The costs of insecurity to each actor would have to be higher than the necessary investments, but many actors have not made that cost benefit analysis. Cyber risk assessments are hard to undertake, with no well-researched methodologies at hand and a lot of higher-level consequences are difficult to foresee. There is also a paucity of data on many of the most serious threats.

In addition, critical infrastructure operators usually don't have to directly bear the full costs of security failures. The sustained interruption of electricity supply caused by a cyber attack (or something else) may prevent or forestall mobilization of a vitally important military unit stationed in the area, but the utility operator bears only a small dollar cost. In the current debate over intellectual property theft by cyber espionage, the argument unfolds at two levels that don't necessarily intersect in terms of responses. One level is the cost to the company, and the other is cost to the national economy. Many companies with sensitive intellectual property, and the professional service firms supporting them, have not moved to prevent their knowledge from being stolen by a foreign government because of a lack of willingness to bear the monetary consequences of implementing high security IT.

Even many militaries are caught up in this conspiracy of circumstance against highly secure computing. Only a small handful of countries can begin to think about paying for a transition to highly secure computing in the defense sectors. Most are already being forced to find new money at a time of shrinking military budgets. They know they will not receive extra money for a re-engineering of their entire IT suite if only because no other military force is doing it. Heavy new expenditure on highly secure computing would only reduce capital investment in conventional military hardware and personnel.

Typically, a market failure—where private markets do not provide goods or services needed by customers or do not provide them in adequate quantities at an affordable price—triggers the question of government intervention.[30] In most market economies, considerable care is taken to craft policies that address the national interest (or public interest) test without unduly constraining innovation and competitiveness in the private sector. But once a government chooses to intervene, the inevitable result—absent a complete course reversal by the private sector—must be some compromise with and by private sector interests. Just how this might play out in particular economies is well beyond the scope of this paper. It is worth noting that the inevitable outcome is an "imperfect policy."

A 2010 study noted some national variations. Having observed an emerging consensus that protection of critical national information infrastructure was no longer a technological problem but one of public policy (economics and regulation), it went on to note that "the USA is regulating cybersecurity in the electric power industry, but not in oil and gas, while the UK is not regulating at all but rather encouraging industry's own efforts." It reported that "some European governments are intervening, while others are leaving cybersecurity entirely to plant owners to worry about."[31] Any government intervention for more generalized application of highly secure computing technologies will not be received well by some industry leaders in most countries.

The traditional IT and IT security industry is not likely to be a friend of "new computing" either. Even if such computers, systems and standards were introduced only in critical areas, that intervention would be regarded as

The necessary changes are expensive, and the choices lie largely in the traditionally free and largely unregulated market.

29 It has to be mentioned that high security computing is also less expensive in some other respects. It does not have to be maintained and updated as often, and there is far less need for upgrades to novel versions. Many high-security researchers also claim that there will not be any decline in speed or functionality. But the overall cost-benefit comparison cannot be estimated properly as long as these systems are not implemented.

30 See Peter Kell, "Market Failure: When Should Policymakers Act?," Per Capita Policy Exchange 2009. Kell was Deputy Chair of the Australian Consumer and Competition Commission.

31 Ross Anderson and Shailendra Fuloria, "Security Economics and Critical National Infrastructure" in Tyler Moore, David Pym and Christos Ioannidis,*Economics of Information Security and Privacy*, Springer, Dordrecht NL, 2010.

a threat by suppliers, since they would demonstrate how insecure and obsolete much of their traditional equipment is. They would be challenged, in particular as some of these new competitors might want to expand into the broader consumer market. As a result, counter-disruptive lobbyism is a problem. For example, in the United States, the TechAmerica web page on cybersecurity reveals the intensity of differences between the industry lobby group and the U.S. Congress and Obama administration, as well as with the European Union.[32] While all this is normal behavior for market economies in democratic systems, the end result is slow progress towards the goal of higher security.

Most senior politicians—or senior decision makers at large—are not as familiar with the technologies as the situation seems to demand.

Many strategists and computer scientists are concerned about this slow, incremental pace of reform, in part because alternative approaches are not the subject of the economic study they need.[33] In the absence of detailed studies, we are inclined to believe that a new mass market for highly secure computing technologies could be generated, with high returns and strong growth, once operational. But to initiate this market, clear policy signals would be required. Political forces would have to indicate that they would require the implementation of high security IT in critical areas. If that doesn't happen, there may be no change.

A few options to influence the market were canvassed at a conference in February 2013: international tariffs, regulations, taxes, insurance, legal liability, reputation damage and criminalization are among the means commonly used to shape markets and to compensate for negative externalities.[34] Another approach could be to simply standardize and produce high security IT for particular niches, which cannot do without it anyway—such as militaries, aerospace or nuclear power plants—and modify those systems for environments with lower security needs.

But this is the point at which policy failure plays a crucial role. Most senior politicians—or senior decision makers at large—are not as familiar with the technologies as the situation seems to demand. Nor are many users as literate in the area of high security computing as they need to be. Policy makers may prefer discussions on "soft" measures such as information sharing or international norms and contracts. This sort of activity is essential, but it should not be taken as a substitute for discussion of the economic and technological issues at the root of the problem.

Yet another problem arises from blurred definitions or empirical uncertainties about the scale of the threat, enabling some to interpret reality in their particular fashion and to render their product as the ideal solution.[35] An antidote to many of these problems would be to insist on security audits undertaken by independent, high-end red teaming to rigorous standards, with the results published—as is now the case in many other safety-critical areas such as aviation or medical technology and pharmacology. But, again, this would entail interference with the market, and it would require strong, independent, knowledgeable politicians.

Anyone seeking to implement new policies will need to work through the firmly established approach of multi-stakeholder consultations. Yet it will be important that such consultations not lose sight of the main goal (highly secure computing) and compromise it by settling for lowest common denominator solutions. It is important to diffuse decision-making among parties with legitimate interests, but at some point a paradigm shift to highly secure computing will require political leaders to ignore some part of the market's current shared opinions. They will need to be

32 See http://www.techamerica.org/public-policy-advocacy/all-industry-priorities/cybersecurity/.

33 A part of it is even well researched in its own discipline of computer science called "Economics of IT-Security" (EIS). This research is still focussed very strongly on petty cyber crimes and thus not applicable to the debate around high level attackers and international cyberstability.

34 John Mallery, "Rebalancing Cyber Defense and Offense: Can incremental technical evolution achieve sufficient work factor impacts or are clean-slate transformational architectures required?," Presentation at the Expert Workshop on "Advanced Strategies in Cybersecurity," Federal Foreign Office, Berlin, February 13, 2013. Explicit quotation permitted.

35 As the famous computer scientist Morrie Gasser already noted in 1988 in his chapter "False Solutions Impede Progress" [*sic*]: "Since few people have a good understanding of security, security fixes are particular subject to snake-oil salesmanship" (p. 12). (see: Morrie Gasser, Building a Secure Computer System, New York 1988).

tough enough to make controversial, costly decisions about technical settings that will run into strong opposition.

Possible Responses

The critique we are making may sound harsh. We do not mean to suggest that the concerns of the traditional market or widespread dependencies on existing systems are inconsequential. But in times of rising cyber tensions and growing numbers of attackers and attacks, the international debate needs to be more informed about options. Highly secure computing is an important option. It represents a new pathway towards a privacy-preserving, peaceable, feasible, more reliable and possibly even more profitable path to cybersecurity.

The answer to many global cybersecurity dilemmas may be found in the new disruptive technology of highly secure computing. It is within reach, and it has to happen anyhow. States, communities and corporations would be remiss in not demanding it. There are providers out there. Some new research projects are already underway, investigating a shift at least from a technical point of view.

For example, in 2010 and 2011, the Defense Advanced Research Projects Agency (DARPA) launched new programs to explore technological options that did not depend on compatibility with legacy architectures and operating systems. The DARPA "CRASH" program is most notable among these efforts.[36] However, as this paper aims to demonstrate, such efforts have been made before. Many ideas have been laid down decades before the current crisis. If the combined mechanisms of market pressures and policy failures are not addressed clearly, honestly and openly, it is unlikely that any effort at substantial reform of our insecure IT environments will actually ever take off. Disruptive innovation may need to be initiated and accompanied by disruptive regulation.

As suggested above, the responses will vary from country to country. It is worth recalling that views of the cybersecurity landscape look very different from various capitals. What will work well in one country may prove unworkable in others. Above all, we are obliged to observe that for the majority of countries, the response may be very different from that which works in the United States. The political priorities and social values will shape the responses. There is new debate everywhere about these values. Scientists in the United States are reserving the right to produce NSA-resistant encryption capability. Europe and the United States appear to be even further apart on these issues than they were a year ago, not least because of the Snowden revelations. And China is drawing up new plans to strengthen its domestic cybersecurity industry, which today is relatively weak compared with its U.S. equivalent.

A number of activities could be envisioned to realize this new paradigm of highly secure computing and to overcome market pressures and policy failures. Whether they can be adopted on any sort of consensus basis within the major national jurisdictions is yet to be seen. Here are some priority courses of action:

1. Highly secure computing has to be prioritized in specifications of critical national infrastructure. Germany is currently about to determine some first strategic steps to this end and incentivize corresponding responses from German industry;
2. Risk assessment methodologies have to be developed or refined to enable a broader view of the overall and higher-order costs and consequences of cyber insecurity;
3. Honesty regarding cyber incidents and the state of cybersecurity can be enforced by laws on incident disclosure, by regular checks and by rigid penetration testing according to security demands;
4. National security decision-makers have to be more open with the public about the implications of active defense and overly intrusive exploitation (espionage);
5. Innovation cycles have to be used to enhance security by detailing high security specifications as new demands;
6. Money from other technology projects aimed at security-relevant areas might be redirected to high

Highly secure computing has to be prioritized in specifications of critical national infrastructure.

36 See: http://www.darpa.mil/Our_Work/I2O/Programs/Clean-slate_design_of_Resilient_Adaptive_Secure_Hosts_%28CRASH%29.aspx (accessed 28th of March, 2013)

As long as the price signal can be clear and appropriately foreshadowed, based on consultation with stakeholders, the private sector will adjust in a way that delivers a more acceptable balance between commercial and public interest.

security IT projects, as the DHS research priorities of 2009 suggested in the case of the United States;

7. Computer science has to receive incentives to invest more in research on highly secure computing;
8. The market potential of high security, verifiable IT has to be assessed more consistently by economists and business advisers;
9. Policy makers and decision-makers from industry need to become more knowledgeable about the economics of highly secure computing.

The Diplomatic Dimension

It is important to understand the international dimension of the possible elevation of the paradigm of highly secure computing to a central position in policy. We asserted early in the paper that active defense was ineffective, controversial and destabilizing, and that we need more attention to defensive options. We believe that the idea of highly secure computing might become a unifying defensive principle of cyberspace cooperation.

If put forward as a common international goal, highly secure computing could help to ease the tensions created by the current, prevalent active defense approaches of several leading countries. Current approaches have seen a resort to cyber nationalism, with like-minded nations trying to solve the problem for themselves inside their own camp or alliances, making more universal international agreements on significant issues less likely. A side effect of this nationalism and alliance building has been to resort to strategies of technological sovereignty. There is increasing mistrust in some countries of "foreign" computers, networks or components. While this is understandable, we have through such lines of thinking all too readily fallen back into the paradigm of East vs. West. Ironically, the indivisible security promised by the end of the Cold War no longer appears to be the goal even as we move more deeply into this most globalized and borderless domain.

Looking to the future, we have to find a new common pathway. There are several drivers for this need. The single most persuasive one is the high level of economic interdependence among the major economies. There are technological, economic and political reasons for global standards. We contend that a drive for cooperative, highly secure computing technologies as a major plank of international strategy by all states would, in and of itself, have a significant and immediate dampening effect on existing inter-state tensions in cyberspace.

What should states do next? Securing cyberspace may not be as important an international priority as mitigating global climate change, but we can learn from the way that process has unfolded. We will see political

There is an urgent and compelling diplomatic need for sustained and productive intergovernmental conversation, including industry stakeholders and civil society, on what those new criteria might be.

agendas that will be every bit as contested and will replay the same arguments about over-regulation and retarding the economy. Yet the domestic divisions and legislative gridlock inside different countries on the climate change issue do not speak to the seriousness of that problem at the global level or the determination of the majority of states to act. Similar domestic divisions and legislative gridlock on issues of high security computing, or the principled positions of disputing parties inside different countries, do not invalidate the importance of that goal at the global level either. As with climate change mitigation policies, such as a carbon tax, as long as the price signal can be clear and appropriately foreshadowed, based on consultation with stakeholders, the private sector will adjust in a way that delivers a more acceptable balance between commercial and public interest.

The international community should start talking about the possible value of a price signal to the ICT industry, regardless of the flag of registration of the corporations. In the future, products and systems that continue to perpetuate inherent low security might face administrative discrimination in the form of higher taxation or legal liabilities. In some jurisdictions, a policy like that may prove unhelpful. But other countries will go down that path.

The first departure point may be more explicit recognition of the slow pace of development of existing international arrangements. For example, the Common Criteria Recognition Agreement, which helps to set international industry security standards, counts only 26 countries as members, of which 17 are certificate authorizing members. In the 2012 Vision Statement issued by the Common Criteria Management Committee, all members agreed that "The general security level of general ICT COTS certified products needs to be raised without severely impacting price and timely availability of these products."[37] This is probably not where the international community needs to be—only 27 countries agreeing to the current market position. The vision statement did hold out the idea that "certification may not always be sufficient for acceptance of certified products for use in a particular context. Other requirements or regulations may also be applicable."

We believe there is an urgent and compelling diplomatic need for sustained and productive intergovernmental conversation, including industry stakeholders and civil society, on what those new criteria might be. The idea is for them to promote urgent pressure for a disruptive innovation towards highly secure computing and for a recommitment to the principle of common, indivisible security.

37 CCMC, "Vision statement for the future direction of the application of the CC and the CCRA," September 1, 2012, http://www.commoncriteriaportal.org/files/ccfiles/2012-09-001_Vision_statement_of_the_CC_and_the_CCRAv2.pdf.

EastWest Institute Board of Directors

OFFICE OF THE CHAIRMEN

Ross Perot, Jr. (U.S.)
Chairman
EastWest Institute
Chairman
Hillwood Development Co. LLC
Board of Directors
Dell Inc.

Armen Sarkissian (Armenia)
Vice Chairman
EastWest Institute
President
Eurasia House International
Former Prime Minister of Armenia

OFFICERS

John Edwin Mroz (U.S.)
President, Co-Founder and CEO
EastWest Institute

R. William Ide III (U.S.)
Council and Secretary
Chair of the Executive Committee
EastWest Institute
Partner
McKenna Long and Aldridge LLP

Leo Schenker (U.S.)
Treasurer
EastWest Institute
Senior Executive Vice President
Central National-Gottesman Inc.

MEMBERS

Martti Ahtisaari (Finland)
Former Chairman
EastWest Institute
2008 Nobel Peace Prize Laureate
Former President of Finland

Tewodros Ashenafi (Ethiopia)
Chairman and CEO
Southwest Energy (HK) Ltd.

Jerald T. Baldridge (U.S.)
Chairman
Republic Energy Inc.

Peter Bonfield (U.K.)
Chairman
NXP Semiconductors

Matt Bross (U.S.)
Chairman and CEO
IP Partners

Robert N. Campbell III (U.S.)
Founder and CEO
Campbell Global Services LLC

Peter Castenfelt (U.K.)
Chairman
Archipelago Enterprises Ltd.

Maria Livanos Cattaui (Switzerland)
Former Secretary-General
International Chamber of Commerce

Michael Chertoff (U.S.)
Co-founder and Managing Principal
Chertoff Group

George F. Russell, Jr. (U.S.)
Former Chairman
EastWest Institute
Chairman Emeritus
Russell Investment Group
Founder
Russell 20-20

Ramzi H. Sanbar (U.K.)
Chairman
SDC Group Inc.

Ikram ul-Majeed Sehgal (Pakistan)
Chairman
Security & Management Services Ltd.

Amb. Kanwal Sibal (India)
Former Foreign Secretary of India

Kevin Taweel (U.S.)
Chairman
Asurion

Amb. Pierre Vimont (France)
Executive Secretary General
European External Action Service
Former Ambassador
Embassy of the Republic of France in Washington, D.C.

Alexander Voloshin (Russia)
Chairman of the Board
OJSC Uralkali

Amb. Zhou Wenzhong (China)
Secretary-General
Boao Forum for Asia

NON-BOARD COMMITTEE MEMBERS

Laurent Roux (U.S.)
Founder
Gallatin Wealth Mangement, LLC

Hilton Smith, Jr. (U.S.)
President and CEO
East Bay Co., LTD

CO-FOUNDER

Ira D. Wallach* (U.S.)
Former Chairman
Central National-Gottesman Inc.
Co-Founder
EastWest Institute

CHAIRMEN EMERITI

Berthold Beitz* (Germany)
President
Alfried Krupp von Bohlen und Halbach-Stiftung

Ivan T. Berend (Hungary)
Professor
University of California, Los Angeles

Francis Finlay (U.K.)
Former Chairman
Clay Finlay LLC

Hans-Dietrich Genscher (Germany)
Former Vice Chancellor and Minister of Foreign Affairs

Donald M. Kendall (U.S.)
Former Chairman and CEO
PepsiCo. Inc.

Whitney MacMillan (U.S.)
Former Chairman and CEO
Cargill Inc.

Mark Maletz (U.S.)
Chairman, Executive Committee
EastWest Institute
Senior Fellow
Harvard Business School

DIRECTORS EMERITI

Jan Krzysztof Bielecki (Poland)
CEO
Bank Polska Kasa Opieki S.A.
Former Prime Minister of Poland

Emil Constantinescu (Romania)
President
Institute for Regional Cooperation and Conflict Prevention (INCOR)
Former President of Romania

William D. Dearstyne (U.S.)
Former Company Group Chairman
Johnson & Johnson

John W. Kluge* (U.S.)
Former Chairman of the Board
Metromedia International Group

Maria-Pia Kothbauer (Liechtenstein)
Ambassador
Embassy of Liechtenstein to Austria, OSCE and the UN in Vienna

William E. Murray* (U.S.)
Former Chairman
The Samuel Freeman Trust

John J. Roberts (U.S.)
Senior Advisor
American International Group (AIG)

Daniel Rose (U.S.)
Chairman
Rose Associates Inc.

Mitchell I. Sonkin (U.S.)
Managing Director
MBIA Insurance Corporation

Thorvald Stoltenberg (Norway)
President
Norwegian Red Cross

Liener Temerlin (U.S.)
Chairman
Temerlin Consulting

John C. Whitehead (U.S.)
Former Co-Chairman
Goldman Sachs
Former U.S. Deputy Secretary of State

* Deceased

EastWest Institute Policy Report Series

2013

Afghan Narcotrafficking
A Joint Threat Assessment
Policy Report 2013—1 [EN | RU]

The Path to Zero
Report of the 2013 Nuclear Discussion Forum
Policy Report 2013—2

Threading the Needle
Proposals on U.S. and Chinese Actions
on Arms Sales to Taiwan
Policy Report 2013—3

Measuring the Cybersecurity Problem
Policy Report 2013—4

2012

Bridging the Fault Lines
Collective Security in Southwest Asia
Policy Report 2012—1

Priority International Communications
Staying Connected in Times of Crisis
Policy Report 2012—2

2011

Working Towards Rules for Governing Cyber Conflict
Rendering the Geneva and Hague Conventions in Cyberspace
Policy Report 2011—1 [EN | RU]

Seeking Solutions for Afghanistan, Part 2
Policy Report 2011—2

Critical Terminology Foundations
Russia-U.S. Bilateral on Cybersecurity
Policy Report 2011—3

Enhancing Security in Afghanistan and Central Asia through Regional Cooperation on Water
Amu Darya Basin Consultation Report
Policy Report 2011—4

Fighting Spam to Build Trust
China-U.S. Bilateral on Cybersecurity
Policy Report 2011—5 [EN | CH]

Seeking Solutions for Afghanistan, Part 3
Policy Report 2011—6

2010

Economic Development and Security for Afghanistan
Increasing Jobs and Income with the Help of the Gulf States
Policy Report 2010—1

Making the Most of Afghanistan's River Basins
Opportunities for Regional Cooperation
Policy Report 2010—2

The Reliability of Global Undersea Communications Cable Infrastructure
Policy Report 2010—3

Rights and Responsibilities in Cyberspace
Balancing the Need for Security and Liberty
Policy Report 2010—4

Seeking Solutions for Afghanistan, Part 1
Policy Report 2010—5

Building Trust
Delivering Solutions

The EastWest Institute seeks to make the world a safer place by addressing the seemingly intractable problems that threaten regional and global stability. Founded in 1980, EWI is an international, non-partisan organization with offices in New York, Brussels, Moscow and Washington. EWI's track record has made it a **global go-to place for building trust, influencing policies and delivering solutions.**

–

Learn more at **www.ewi.info**

EastWest Institute

EWInstitute
EastWestInstitute