Bundeskriminalamt

HERBST-TAGUNG BKA 2013 AUTUMN CONFERENCE

Cybercrime –

Bedrohung, Intervention, Abwehr

BKA-Herbsttagung vom 12. - 13. November 2013

Cybersecurity – strategic-political aspects of this global challenge

Full version

Michael Daniel

Special Assistant to the President of the United States of America and Cybersecurity Coordinator, White House

OPENING COMMENTS

Good morning everyone. Thank you for the kind introduction**.** It's a pleasure to be here with you here in Wiesbaden for the BKA's annual conference – particularly this one given its focus on "**Cybercrime: Threat, Intervention, Defense**." I'd like to congratulate our German hosts for putting on such an excellent event.

My name is Michael Daniel, and I currently serve as Special Assistant to the President and Cybersecurity Coordinator at the White House.

In my role, I lead the United States Government's development of national cybersecurity strategy and policy and oversee the implementation of those policies on behalf of President Obama.

One of the great parts of this job is to getting to engage and listen to a diverse range of representatives from across government, the private sector, and academia. I've particularly been looking forward to this conference; this is my first trip to Europe in my capacity as the Cybersecurity Coordinator.

Today, I would like to provide an overview of some of the U.S. Government's current thinking on cybersecurity, including our priorities, areas of potential challenges and opportunities, and how the United States and Germany can work together to improve our collective security in cyberspace.

THE "NEW NORMAL"

But first, I'd like to briefly talk about the challenges we face in cyberspace. As all of you know, cyber threats pose a significant problem for governments and businesses alike. From the White House perspective, three trends make the cyber threat particularly troubling:

• First, the threat is becoming broader and more diverse – as we hook more and more items up to the Internet, the potential vectors for attack are growing exponentially, making the area we need to defend ever bigger. And we are continually connecting new and different things to the Internet – think everything from cars to coffee makers to distributed sensors -

so the problem of defense is even more challenging than "simply" protecting desktops connected by wires.

• Second, the threat is becoming more sophisticated – malware is getting harder and harder to detect, and it does more varied kinds of things. At the same time, you no longer have to be a coder to use malware. Not only are malicious developers making malware easier to use, in some cases, cybercriminals have established on-line help desks, so that if your malware doesn't work, you can call and get help.

• Third, the threat is becoming more dangerous – malicious actors are showing an increasing willingness to be more destructive in their activities, as we have witnessed with the attack against Saudi Aramco last year and South Korean banks earlier this year.

But what is ultimately more concerning is how "normal" these threats are becoming. The new normal is not massive power outages or train traffic grinding to a halt nationwide—those kinds of things are not "normal." At least, not yet. Rather, these trends are leading to a "new normal" that is less flashy than a Hollywood action movie, but still very troubling: persistent intrusions, violations of privacy, thefts of business information, and degradation and denial of service to legitimate entities trying to do business or getting their message out on the Internet.

NO INTERIOR TO CYBERSPACE

As we think about how to manage these threats, we have to keep in mind one unique characteristic of cyberspace. Traditionally, the argument has been that cyberspace has no borders, and that's both a strength (the free flow of information drives huge economic benefits) and a problem (it allows malicious actors great freedom of movement).

But I would argue that such arguments are not entirely correct. There are borders and boundaries everywhere in cyberspace. Every place there is a firewall or a connection point, there is a border. Instead, what cyberspace lacks is an interior – there is no "inside" to our network spaces. Everyone effectively "lives" at the border. We are all connected through cyberspace, and that interconnectedness means that everything and everyone touches an edge or a border in some fashion.

And this reality has some profound implications for how we organize ourselves a society to protect ourselves in cyberspace – and how I try to carry out my cybersecurity role. For example, in the physical world, we assign the mission of "border security" to the national government. But if everyone lives right at the border in cyberspace, then it's not physically possible to assign the "border security" mission to just one group or element of our society, even the national government. It becomes a shared mission, one that everyone in a country or society has a role in. And it means that conventional ways of thinking about threats need to change as well. For example, in many countries, citizens expect national governments to deal with "external" threats, while local governments tackle limited "internal" threats, like crime. But we have seen states taking malicious action through locally based servers and petty criminals stealing money from abroad; we can no longer simply use "external" and "internal" as the basis for allocating responsibility for action.

GUIDING PRINCIPLES

So how do we improve our collective security in a "new normal" of daily intrusions against individuals, businesses, and governments? If you were hoping that I would now supply the answers to these questions, I am afraid I am going to have to disappoint you. I don't have those complete answers yet, nor do I think anyone does. However, I would like to highlight some of the principles we are following in the United States as we work to address this challenge.

Compromises Are Inevitable; Plan for Them. In living with this "new normal," we cannot be surprised when intrusions and outages occur. Instead, we must be prepared. Businesses and governments alike should develop and test their cybersecurity incident response plans; use modern network defense best practices and technologies; and continuously monitor their networks under the assumption that they have been breached. And everyone should have contingency and fallback plans in place with service providers should all else fail.

Information Must Be Shared, Frequently and Rapidly. Cybersecurity is a shared challenge and the international community has a shared responsibility in working together to address it. To do so, we all must be willing and able to share information about the respective threats we face. This requires collaboration at all levels: between governments; between government and industry; and between companies in the private sector. After all, the threats that we face today may be the threats you face tomorrow.

Teamwork is a Requirement. In speeches back home, I often say: "cybersecurity is a team sport." What I mean is that no single entity in our country can address this issue alone. Everyone, from the private sector to law enforcement to homeland security to civil society, has a role to play. This is true in the United States and I believe it is true internationally – if we are only as strong as the weakest link in our interconnected networks, we each share responsibility for the safety and security of one another.

Network Defense First. The risk of misattribution, miscalculation, and escalation in cyberspace is very real. As a government, we consider all of our cybersecurity and network defense activities against their possible foreign policy implications and our desire to establish international norms of acceptable behavior in cyberspace. We don't want our response to a minor cyber incident to harm our relationships with other nations or worse, result in physical conflict. As a result, we will undertake network defense activities first and work hard to make these solutions effective before using other means of dealing with malicious activity.

Protect Privacy and Civil Liberties. The United States firmly believes cybersecurity and privacy are mutually reinforcing, not in competition. Done properly, cybersecurity protects privacy and civil liberties by strengthening the networks and systems that contain personal information—and we are taking steps to make that vision a reality. We are building protection for personal data into our cybersecurity framework for critical infrastructure; ensuring that our network defense actions reflect our commitment to protecting the privacy and civil liberties of the users of those networks; and engaging privacy advocates and other key stakeholders on discussions on how to safeguard privacy and civil liberties while supporting business and enhancing security. We also insist on strong privacy protections in any cybersecurity legislation that our Congress considers. All of our partners, both in the United States and internationally, must have confidence in our ability to protect information you choose to share with us.

PUTTING THE PRINCIPLES IN PRACTICE INTERNATIONALLY

We are putting these principles into practice across all of our cybersecurity efforts – both domestically and internationally.

Protecting Critical Infrastructure

First, we are working to strengthen the cybersecurity standards and practices in our critical infrastructure sector. As a key step in this effort, earlier this year, President Obama signed an Executive Order directing several actions aimed at exactly this goal. In particular, the Executive Order strengthens the U.S. Government's partnership with critical infrastructure owners and operators to address cyber threats through information sharing, the protection of privacy and civil liberties, and the development of a framework of cybersecurity best practices and standards.

We believe that governments have a clear role in helping private sector companies help themselves, especially when it comes to critical infrastructure owners and operators. To that end, the Executive Order requires the U.S. government to increase its efforts to share actionable information with those who need it the most – network defenders, companies, and other governments. We have already started this and want to do more of it. For example, we have shared hundreds of thousands of signatures and indicators of malicious cyber activity with the private sector and over a hundred nations just in the past six months. It also incorporates strong privacy protections by mandating that Federal agencies follow the Fair Information Practice Principles or FIPPs when implementing their cybersecurity actions.

But we recognized information sharing alone would never be enough; we also needed to raise the bar for cybersecurity in the United States. So, the Executive Order also directed the creation of a framework of cybersecurity best practices and standards for critical infrastructure. Over the last 9 months, the U.S. government has collaborated with the private sector to develop this framework. Let me be clear: the framework is not a scientific breakthrough in cybersecurity. It is actually more basic, outlining the best practices that many firms already do. What it does do, however, is provide a structured way for companies to think about their cybersecurity risk, determine their current level cybersecurity, and then decide what they would like their level to be. The framework then points to the standards and practices that, if implemented, will get companies to their desired cybersecurity level.

We recently completed the preliminary draft of this framework. We think it is an excellent start, but we know it can and will be improved upon in the future. As part of the process for finalizing the preliminary draft, we have asked for companies, industry sectors – in fact, almost anyone – to

implement the framework and provide us with feedback on what works and what does not. That request extends internationally as well – we welcome feedback from any government or any multinational company that chooses to provide it. As I said before, the United States does not have all the answers – by working with our international partners, we know we can achieve more together than we ever could individually.

Norms Development and Foreign Policy

Second, we are working to integrate cybersecurity as a core element of our foreign policy relationships with other countries. Since cybersecurity is a shared responsibility, it is not exclusively a domestic issue.

In cyberspace, as elsewhere, states have a special responsibility to protect their own national security and promote peace and stability with other nations. Consequently, we continue to engage our Allies and partners worldwide to solidify norms of cyber behavior – what states and other actors should and should not do in cyberspace – and to ensure the Internet remains open, interoperable, secure, reliable, and stable, following the principles outlined in the U.S. *International Strategy for Cyberspace*. In doing so, we are striving to create an environment in which everyone can benefit from cyberspace, in which cooperation is encouraged, and in which there is little incentive for states to disrupt or attack one another.

But the truth is that actions speak louder than words. So to promote the norms we want, we must take the steps to make them a reality. We need to move to an environment where all countries routinely and quickly respond to requests for assistance in mitigating cybercrime and other malicious cyber activities emanating from their territory. The United States is committed to working with the international community to build the processes and capacity needed to respond to malicious activity through such collective action.

Internet Governance

Third, the United States remains steadfast in our support for an Internet governance model that supports international trade and commerce, strengthens international security and fosters free expression and innovation. We strongly believe that proposals advocating international regulation to

curb the open and free nature of the Internet would slow the pace of innovation and economic development and could lead to unprecedented control over what people say and do online. Such proposals play into the hands of repressive regimes that wish to legitimize inappropriate state control of content. Instead, we believe that governments, the private sector, and civil society all have an important voice on the future of the Internet. If we truly believe that the path to economic growth and prosperity is through an open, connected world, we must strengthen—not weaken—the multistakeholder institutions that are critical to the management and administration of the Internet itself.

Law Enforcement Cooperation

Fourth, we believe that we must increase our ability to disrupt malicious activities in cyberspace. In order to achieve this goal, we must deepen our law enforcement cooperation across the international community, but particularly with Germany and other European allies. The United States and Europe have had several successes in recent years:

- We established an EU-US Working Group on cybersecurity and cybercrime to identify common goals and actions to achieve those goals;

- We have had success in getting more countries to ratify the Council of Europe Convention on Cybercrime and make it a truly global instrument for combatting cybercrime; and

- Last year the United States and the EU launched the Global Alliance Against Child Sexual Abuse Online;

All of these are notable achievements. But as technology continues to evolve, our legal responses must evolve with it. Issues such as data protection, law enforcement access to data across borders, or information sharing between the public and private sector create new challenges for our law enforcement cooperation. We can, and must, ensure that our cooperation meets those challenges in order to address the ever-evolving threat from cybercriminals and non-state actors.

Capacity-Building

While I've talked at length about the United States' cybersecurity efforts, we are mindful that many countries are still working to develop the industries, technologies, and connectivity necessary for economic development in the 21st century. To bridge that gap, we are committed to connecting more people around the world to the digital future. The United States believes that expanded global access to telecommunications and broadband services—combined with an inclusive, multistakeholder-driven Internet governance model—remains the best path towards economic growth that benefits everyone.

And finally, we are committed to assisting developing nations around the globe build their cybersecurity capacity. Across the U.S. government, we have established programs to help governments create cybersecurity policies and programs from the ground up. These programs help address any number of needs, such as developing rule of law in cyberspace; drafting national cybersecurity strategies; and creating computer emergency response teams. As just one example, the U.S. State Department has spent significant time and effort working with Senegal and Ghana to build long-term cybersecurity partnerships between the United States and fourteen
states in West and Central Africa.

We are only one country, however, and we do not have unlimited resources. Therefore, we are eager and willing to work with other nations on awareness-raising, legal and technical training, and other initiatives that will bolster our collective pursuit of an open, interoperable, secure, and reliable cyberspace.

U.S.-EUROPEAN CYBER COOPERATION

I would be remiss in giving this speech if I did not emphasize how much the United States values our cybersecurity partnership with Europe – and particularly with Germany. You have been, and will continue to be, a key ally in building a more safe and secure cyberspace:

- As I mentioned above, on cybercrime, our law enforcement agencies have a long-standing and deep cooperative relationship and continue to work together on investigations and prosecutions.

• On incident response, our computer emergency response teams work together regularly to share threat information and address malicious cyber activity. In particular, we were deeply grateful for the timely and immediate assistance the German government provided earlier this year when we asked for help with ongoing denial of service attacks against our banks and financial sector.

• On foreign policy, our diplomats continue to be the staunchest of allies for our "like-minded" views on the applicability of international law to cyberspace and norms of behavior for states in cyberspace.

We are committed to this partnership. While the United States and Germany at times differ in our opinion of the best way to build a more safe and secure cyberspace, we do agree on the importance of this mission. We cannot and must not lose sight of the fact that our cooperation and continued dialogue serves to strengthen and secure cyberspace for both our citizens.

CONCLUSION

I'd like to conclude with a few final thoughts:

• First, while we must continue to be mindful of the threats we face, we must all improve our collective cybersecurity capability through collaboration and partnership.

• Second, solving our cybersecurity challenges will not be easy and will require persistence from all of us. But as President Obama said in his State of the Union address earlier this year: "We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."

• Finally, the Information Age has only just begun. While the issues we face are complex and challenging, we have an opportunity now to put the foundation in place for a safer and more secure future. I, for one, look forward to that challenge.

Again, I'd like to thank our hosts of this conference for putting on such a wonderful event. I appreciate the opportunity to speak to all of you and look forward to our continued work to meet these challenges. Thank you.