An Interview with Marina Kaljurand, former Minister of Foreign Affairs of Estonia

You were the Estonian Ambassador to Russia during the 2007 cyberattacks against your country. Please describe those attacks—the effects of the attacks, and what Estonia learned from that experience.

Kaljurand: Those were the first explicitly political cyberattacks against an independent, sovereign state in history. If put into today's context, the attacks were not very sophisticated—even primitive. But back then, they were very disturbing. By that time, Estonia already had widely established internet and e-services, and an e-lifestyle; when those services were interrupted—mainly in the banking sector—it was highly disruptive. As to the effects of the attacks? They did not kill anybody, they were not destructive. They were highly disruptive to our lives though.

We have learned several lessons: First, you have to have your house in order, which means that you need an appropriate legal framework. You have to have strategies and action plans in place that clearly describe who is responsible for what. What are the obligations? What are the timeframes?

Second, we learned that efficient cybersecurity depends on an all-nation approach. Governments must of course have a central role in data security, but there must be an all-nation approach based on cooperation with other stakeholders, including the private sector, which plays a big role in cybersecurity and in providing internet services to the people. In Estonia, we were lucky to have assistance from the private sector from the very beginning of the attacks. Information and technology (IT) experts from the private sector volunteered to assist and support the government. A year later, a volunteer Cyber Defense League was created within the private sector, which symbolized the public–private partnership in real life, in practical terms. Today the League continues to work in very close partnership with the Government. Its members have security clearances and cooperate on a regular basis.

This interview was conducted by Mr. Michael Miklaucic in September 2017.

Partnership with industry is crucial, as is cooperation with academia. Although at the United Nations we have agreed that international law governs cyberspace—whether discussing countermeasures, sovereignty, or jurisdiction—the issues are very complicated; more complicated than most realize. So here, the expertise of genuine legal scholars from academia is important. Also necessary is cooperation with technical, and IT experts. That is the all-nation approach as we call it; where government has a leading role, but cooperates closely with other stakeholders.

The third lesson we learned is that cyberspace does not have borders. That means international cooperation is important. That is one of the reasons why we [Estonia] have been so vocal in international organizations, and have been very strong supporters of close, international cooperation; starting with international law, confidence building measures, capacity building measures, and all other efforts.

Given the inherent problem of attribution in cyberattacks, how can countries retaliate? And what are the principles that should govern retaliation against cyberattacks?

Kaljurand: The same principles that govern us in our offline life should govern us in the online dimension. We have the principles of international law—we have the UN Charter, Article 51 of which establishes for all countries the inherent right of self-defense—these principles are in place. In the case of cyberattacks, we should be guided by the same principles.

How does that work in practice? We are just now taking the first steps. Lawyers are interpreting and countries are starting to apply international law to the cyber domain. One of the measures of retaliation we used in 2007 was to put those we ascertained participated in the attacks onto the Schengen Black List.[1] I doubt at that time we really understood how powerful a tool that was. But, it worked. It was noticed. That was our reaction then. Other states have taken additional countermeasures. State practice in this regard is still developing and it will take time before we can say that we have effective and appropriate rules for countermeasures in the cyber sphere. The bottom line is that we have a basis in international law, and the same rules and principles that govern us in real life also apply to cyber.

In terms of state strategy would you advise that resources be invested in minimizing risks, or should states accept the risks and invest in improving resilience?

Kaljurand: There is no single solution. The solution must consist of different elements. If we look at today's cyber incidents, the majority are the results of human mistakes. Awareness-raising, education, and cyber hygiene have important roles, but we need additional measures for effective cybersecurity. For example, several weeks ago international experts discovered theoretical vulnerabilities in the chips of Estonian personal identification (ID) cards. Although the vulnerabilities were theoretical, we are undertaking corrective measures to avoid, or at least minimize the risks. You have to make it as costly and complicated as possible for those who want to attack your systems. Our experts estimate that it might take tens of years and 60 billion Euros to successfully hack Estonian ID cards—that is a high price. Not everyone is ready or able to do that; not everyone is willing to pay that price. This is a form of resilience—a way of making your systems secure. Those who want to attack systems will go for the ones that are more easily accessible or cheaper so that they do not have to expend so much in terms of human and financial resources.

I would also like to underline once again the importance of international cooperation and a common global understanding of what is allowed in cyberspace and what is not. It is important to agree

among states, on the rules and norms of responsible state behavior. For example, reaching a common understanding that it is not acceptable to attack critical infrastructure, particularly financial systems or electoral systems, in peace time, and that appropriate responses will follow any such attacks.

Is that also a strategy for cyber deterrence?

Kaljurand: Professor Joseph Nye recently published an excellent article, "Deterrence and Dissuasion in Cyberspace."[2] In it he defines deterrence as a means of dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefiits. He lists four major deterrence mechanisms: threat of punishment, denial by defense, entanglement, and normtive taboos. In other words effective deterrence has multiple components; I agree we cannot rely on any single component.

I also believe in awareness raising and cyber hygiene. Some cybersecurity companies tell us we should accept that our systems/networks are already violated and compromised, and that we should dedicate financial and human resources to identifying violations and restoring the integrity and safety of the systems/networks. That might be one approach. But on the other hand it is important to teach our people, our employees, and our officials how to behave in the cyber sphere. Here, again, government has a central role cooperating with other entities, bodies, and institutions. Governments have to set the criteria, set the standards, and ensure that the standards are followed. This is another important step in reducing cyber risks.

We all know that it is impossible to eliminate all risks, either online or offline. The risks are different and are becoming more challenging with the development of information and communication technologies (ICTs). And it is the task of governments to minimize the risks, for both online and offline services.

In your view who or what are the most dangerous adversaries today in the cyber world?

Kaljurand: Cyber is a very difficult domain in this regard. It is a sphere which is relatively new, is developing very rapidly, and includes states as well as non-state actors. We have not yet seen cyberterrorism attacks, but we cannot assume we will not see them in the future. We have seen states supporting cyberattacks by private actors within their jurisdictions. We have seen illegal cyber activities by non-state actors. There are multiple players in the sphere, but what I think is important is that we take all of the necessary measures to ensure that cyberspace is ruled by law and by norms. We must ensure there is awareness of those rules, and awareness that if someone violates those rules, measures of retaliation will follow, in the same way as we do in real life.

It has been alleged that Russia, China, North Korea, and their proxies are the perpetrators of many of these cyberattacks. In your opinion, is their use of cyber tools, in any meaningful way, different from our own use of cyber tools?

Kaljurand: Speaking on behalf of my government, we [Estonia] have not hacked any elections, we have not interfered in the political systems of other countries. We are using legal means and, if we have problems with some policies of other countries, we use diplomatic means and do it in accordance with international law and international obligations, whether in the physical or the cyber sphere.

Estonia is a world leader in the development of e-government. Do you think that makes Estonia more or less vulnerable to cyber aggression?

Kaljurand: I think both. More vulnerable in the sense that we depend on internet services, which increases our cyber vulnerability. Some countries might not even notice when they are under cyberattack, but in our case, it was and will be acutely noticed. The 2007 experience showed that a country

that has accepted or adopted an e-lifestyle is more e-vulnerable. So, on the one side, yes we are more vulnerable. At the same time, we are taking cybersecurity very seriously. According to the International Telecommunications Union, Estonia ranks 5th in the world and 1st in Europe in terms of cybersecurity. So we are doing pretty well, but there is room for improvement. Additionally, I would argue that we even have an obligation and duty to be leaders in cybersecurity—for the sake of our people and also because the international community is looking to us. In the end Estonia is the only country in the world to conduct online e-voting and the only country in the world that has opened some of its e-services (digital signature, e-banking, e-taxation) to foreigners through e-residency.

As I said earlier, a vulnerability was discovered in our identity cards. The chip manufacturer sells millions of chips to many other countries, but nobody else reported the vulnerabilities, because they are not using them [the chips] the same way we are using them. So, yes, it makes us more vulnerable but, at the same time, we have to be very good with cybersecurity.

I would like to return to an issue you raised earlier; international law and international cooperation. The United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security—the 2016–17 effort failed. Why do you think the GGE failed, and what steps have been taken since then to fill the gap?

Kaljurand: I have had the honor to serve on the 4th and 5th GGEs. It is absolutely regrettable that the present GGE failed—and I am using the word "failed," because our mandate was to reach a consensus report. We were mandated to look into several questions including emerging threats, norms and rules of responsible state behavior, applicability of international law, confidence building measures, and capacity building measures. We made progress in all of the fields, with the exception of international law. In 2013, the GGE agreed, and it was later adopted by the UN General Assembly and international community, that international law applies to the cyber realm. It was agreed in 2013 and reconfirmed in 2015 that the UN Charter in its entirety applies to cyber (or the use of ICTs). But in 2017, we could not agree to reiterate the assurances of Article 51 of the UN Charter guaranteeing the right of self-defense, countermeasures, and International Humanitarian Law (IHL). This is really, really regrettable.

What will happen next? I think it is too early to say. I think that we need a "cooling down" period. We need some time to look into what happened, why it happened, and where we stand today. Most probably we will have some parallel tracks. The ideological division between countries is so great that I am afraid that, in the UN framework, we will not be able to agree on the applicability of international law in the near future. I am not saying that the UN framework is not important, it is important—it is the only global framework we have, so we should maintain it. Maybe not in 2017, maybe in 2018 or even later. We should continue discussing cyber security in the context of peace and security with all countries that want to be part of the discussion. But we have to be very frank, and know that we will not have conclusive results in the near future, at least not on the applicability of international law. I see it as an awareness raising effort and an educational lesson. We must talk to countries who so far are not paying enough attention to cybersecurity; we have to engage more actively with them. I believe that concrete results on the applicability of international law and norms of responsible state behavior will first be reached within a group of like-minded states. And there are regional organizations. I am sure we can achieve

concrete results within the EU and in NATO. The EU–NATO joint declaration and the recent EU cybersecurity package are proof of that. We should continue discussions among like-minded countries, while at the same time engaging with other states. It is our obligation to explain why our approach to cyber—promoting cybersecurity and cyber stability—is in the interests of all individual nations and the international community as a whole. It is our obligation to convince others that free, open, resilient, stable, accessible, and affordable use of ICTs can contribute to development and a better future for all people.

Can you tell us where the resistance was to the consensus in the most recent GGE?

Kaljurand: The resistance was to mentioning specifically Article 51 of the UN Charter, countermeasures in self-defense and the applicability of IHL.

China has recently taken a proactive role in the cyber domain, holding several conferences at which they articulated a view of cyber sovereignty that differs from the, if you will, Western view. Can you comment on their view of cyber sovereignty?

Kaljurand: The question of sovereignty was also raised by several of the GGE delegations, and yes, we do have different views on that. Our view, that is the Estonian view and my view, is that we cannot talk about absolute authority or sovereignty in international law. By acceding to international conventions—by accepting international obligations—we have already given up some part of our sovereignty. Acceding to the International Covenant on Political and Civil Rights, or any other international convention, imposes obligations on a state that effectively limit its sovereignty. Absolute sovereignty and international law are not compatible. Yet some countries continue to interpret state sovereignty as absolute sovereignty, unlimited by international law, subject only to national laws. That is the main contradiction.

What are the most threatening developments in the cyber domain today?

Kaljurand: The use of cyber by terrorists, which we have not seen yet, but we must anticipate. The Internet of Things brings to the internet and cyber arena many more actors, institutions, organizations, and individuals. Artificial intelligence. On one hand these developments have positive impacts on people, economies, and societies; and on the other hand they introduce additional cybersecurity challenges. We have to face the challenges, we have to get ahead of malicious intentions and actions in cyberspace. Cyber will not disappear. Cyber is here to stay, and smart countries will take maximum advantage of that. PRISM

Notes

[1] The Schengen area is an area comprising 26 European states that have officially abolished passport and all other types of border control at their mutual borders. Persons on the black list of any Schengen area country are denied entry to the entire Schengen area.

[2] Joseph Nye, "*Deterrence and Dissuasion in Cyberspace*," *International Security* 41, no. 3 (Winter 2016–17), 44–71, available at <http://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266>.