President Kaljulaid at CyCon 2019: Cyber attacks should not be easy weapon

NE

ER
Ne
29
12:

President Kersti Kaljulaid. Source: Siim Lõvi/ERR

President Kersti Kaljulaid delivered the opening address at the 11th International Conference on Cyber Conflict (CyCon) in Tallinn on Wednesday morning. Here follows an abridged transcript of her speech.

During the 70-year history of NATO, no ally has actually been conventionally attacked or lost its sovereignty. This is because NATO's collective defense posture – at least in the conventional domain – has been and will remain to be a credible deterrent.

Still nobody dares to cross NATO, as the consequences would be known, clear and devastating.

If we think of some of the basic tenets of the international law system, then yes, international law and organizations have not been able to end all wars and aggression, but everybody clearly knows that when you breach international law then it will be taken up for sure in the UN Security Council. And this always has consequences, and therefore also acts as a deterrent.

For some reason, the same principles remain ambiguous in cyber domain, to say the least, although they shouldn't. Today it is still possible for an adversarial country to carry out a malicious cyber operation, or a number of them simultaneously, and get away with it.

Or almost get away with it, since at least on attribution, a lot of progress has been achieved over the last years. But one of the reasons for this is that cyber still leaves a lot of gray areas, including on how precisely international law applies in the cyber sphere. International law stems from conventions, agreements, and custom but it is still very much up to states themselves to define and to interpret that law.

Therefore, the Estonian position on application of international law in cyberspace is our contribution on further clarifying this issue and leading the way together with other allies.

It's also something that will help our own cyber experts in everyday operations, in drafting our own rules of engagement for possible cyber operations. It might also carry some deterrent effects as we have now more clarity in how we perceive and react to cyber operations in the future.

First of all, as also many states and several international organizations have acknowledged – existing international law applies in cyberspace. Among others, the European Union, NATO, OECD and ASEAN have made similar addresses. Estonia has constantly upheld this position. We believe and state that both the rights and obligations of international law, including those stated in the U.N. Charter, do apply to states when using IT and communication technologies.

I would like to reiterate, when it comes to legal questions of dos and don'ts surrounding state behavior in cyberspace, the answer must be sought from existing international law.

Second, states are responsible for their activities in cyberspace. Sovereignty entails not only rights, but also obligations. States are responsible for their internationally wrongful cyber operations, just as they would be responsible for any other activity based on international treaties or customary international law. This is the case whether or not such acts are carried out by state organs, or by non-state actors, supported or controlled by the state. States cannot waive their responsibility by carrying out malicious cyber operations via non-state actors. If a cyber operation violates international law, this needs to be called out.

Third, states must keep strengthening their own resilience to cyber threats and disruptions, both individually and collectively. Therefore, states have to make reasonable efforts to ensure that their territory is not used to adversely affect the rights of other states.

They should strive to develop means to offer support when requested by the injured state in order to identify, attribute or investigate malicious cyber operations. This expectation depends on national capacity as well as availability, and accessibility of information. As I said here last year, we have to also consider the capacities of different states to be able to control such operations that exploit their infrastructure or systems. Therefore, meeting this expectation should encompass taking all feasible measures, rather than achieving concrete results.

And this also means that further effort must go to cyber capacity building and development cooperation to increase states' capacity to prevent and respond to cyber threats.

I hope that Estonia can serve as a model in partnering with other countries, especially in assisting those that do not have robust enough cyber defence systems. Our attention so far has been to Georgia and Ukraine – countries that face constant malicious cyber operations. Because at the end of the day – our own cyber security also depends on this.

The fourth point: states have the right to attribute cyber operations both individually and collectively according to international law. Our ability and readiness to effectively cooperate among allies and partners in exchanging information and attributing malicious cyber activities has improved.

The opportunities for malicious actors to walk away from their harmful actions with plausible deniability are clearly shrinking. Last year demonstrated that states are able to attribute harmful cyber operations, both individually or in a coordinated manner. It is not something unachievable and endlessly complex. At the end of the day, what is required from the attributing state, is not absolute certainty but what is reasonable. When assessing malicious cyber operations we can consider technical information, political context, established behavioral patterns and other relevant indicators.

More than simply attributing, we must take a stance that harmful cyber operations cannot be carried out without consequences. One good example would be EU's Cyber Diplomacy Toolbox, which foresees a framework for joint EU diplomatic response to malicious cyber activities. Two weeks ago, EU Member States agreed on a horizontal framework which will allow to impose restrictive measures, or sanctions, against malicious cyber operations in similar manner as it is possible for terrorist acts or use of chemical weapons. Several allies have already taken diplomatic steps or set in place economic restrictive measures against adversarial states, or individuals responsible for harmful cyber operations.

And now to the fifth and final point from the Estonian positions. Namely, states have the right to react to malicious cyber operations, including using diplomatic response but also countermeasures, and if necessary, the inherent right of self-defense. Cyber should no longer look like an easy choice of weapons and therefore we must be ready to use deterrence tools.

First and foremost, states must refrain from the threat of or use of force against the territorial integrity and political independence of other states. However, we already know that cyber operations, which cause injury or death to persons or damage or destruction of objects, could amount to use of force or armed attack under the U.N. Charter. We here in Estonia are very much dependent on a stable and secure cyberspace. Such harmful effects could be caused by a cyber operation, which for example, targets digital infrastructure or services necessary for the functioning of society.

And let's not forget – the growing digitalization of our societies and services can also lower the threshold for harmful effects. In order to prevent such effects, states maintain all rights, in accordance with international law, to respond to harmful cyber operations either individually or in a collective manner.

Among other options for collective response, Estonia is furthering the position that states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation. The countermeasures applied should follow the principle of proportionality and other principles established within the international customary law.

International security and the rules-based international order have long benefited from collective efforts to stop the violations. We have seen this practice in the form of collective self-defense against armed attacks. For malicious cyber operations, we are starting to see this in collective diplomatic measures I mentioned before. The threats to the security of states increasingly involve unlawful cyber operations. It is therefore important that states may respond collectively to unlawful cyber operations where diplomatic action is insufficient, but no lawful recourse to use of force exists. Allies matter also in cyberspace.

As you see in many ways there is nothing really that special or groundbreaking. But I do believe that it's really important to get them clearly stated. And I am sure that it certainly doesn't end here. I believe that all states should articulate their positions on how international law applies in cyberspace. We look forward to the fruitful discussions on this issue during new working groups established by the Secretary General of the U.N.

In addition to maturing the perception of existing law, we must put our effort to implement those provisions we have already agreed upon, including norms of responsible state behavior in cyberspace and call out those who undermine our efforts to ensure peace and stability in cyberspace. And we all, governments, civil society and industry, have the responsibility to strengthen the resilience of our societies in the context of fast-evolving digital technologies. And there is actually nothing "silent" in all this although the title of this year´s CyCon might imply that there is. We have to be loud on this element of cyber security.

ERR news is carrying a live link of some of the keynote speeches at the conference on Wednesday and Thursday here.

:ditor: Andrew Whyte

cyber defense ccdcoe cyber attacks president of estonia president kersti kajulaid

cycon2019