INTERVIEW WITH MARTIN LIBICKI

DR MARTIN LIBICKI

Dr Martin Libicki (Ph.D., U.C. Berkeley 1978) has been a distinguished visiting professor at the U.S. Naval Academy and a senior management scientist at RAND since 1998, focusing on the impacts of information technology on domestic and national security. In addition he is a Distinguished Visiting Professor at the U.S. Naval Academy and has been an adjunct at Columbia University and Georgetown University. He wrote two commercially published books, Conquest in Cyberspace: National Security and Information Warfare, and Information Technology Standards: Quest for the Common Byte and has a cyberwar textbook (Cyberspace in War and Peace) at the publisher's (U.S. Naval Institute Press). He is also the author of numerous RAND monographs, notably Defender's Dilemma, Brandishing Cyberattack Capabilities, Crisis and Escalation in Cyberspace, Global Demographic Change and its Implications for Military Power, Cyberdeterrence and Cyberwar, How Insurgencies End (with Ben Connable), and How Terrorist Groups End (with Seth Jones). Prior employment includes 12 years at the National Defense University, three years on the Navy Staff as program sponsor for industrial preparedness, and three years for the GAO.

Dear Mr. Libicki, thank you again for finding time for this interview. We are currently witnessing a very interesting process in which both national and international decision-makers are trying to find most efficient ways to address cyberthreats. Especially in the USA numerous activities regarding domestic and international issues are being undertaken. I would like to talk about them in more details.

In a recent testimony from March 2015 presented before the House Homeland Security Committee, you shared your views on broad range of issues related to information sharing. The main conclusion was that even though this process is of high importance, its implementation itself will not solve all the problems. National cybersecurity is a multidimensional problem. What are the other important elements of this endeavour that should gain attention and be encouraged?

Information sharing is good, but we should not be hung up about the form it takes. Some thoughts:

a. We need an ethos in the Cybersecurity community that makes not sharing unethical. In the medical community, doctors commonly share (anonymised) information about patients as a way of discussing situations and treatment options, both those that worked well and those that did not. In the aeronautics industry all incidents are reported and the U.S. NTSB was instituted as a fact-finding but not fault-finding investigative body.

b. We also need an information-sharing mechanism that can infer indications and warnings of a wide attack from the detection of small ones – but there has to be a great deal of empirical work before we understand how.

There is another issue that I would like to underline here. The machine controls essential to critical infrastructures (such as electric power) should be electronically isolated from the rest of the world and such isolation should be mandated and periodically tested.

In your work you pay a lot of attention to the problem of crisis and its escalation in cyberspace. In this context, I would like to ask you following question. It is a well-known fact that NATO is currently looking for an "adequate" answer to cyberattacks, both the ones which can be treated as the acts of cyberwar and the ones which are below the cyberwar threshold. During the CYBERSEC 2015 Conference, one of the speakers pointed out that in order to have a chance to respond to cyberattacks in a proportional way, the Alliance must develop offensive cyber capabilities. Otherwise, we might end up with conventional tools only, while choosing reaction. What do you think about this approach in context of your research?

A proportional response is itself a reaction. Two overarching issues must be addressed in the context of NATO. First, what can NATO countries tolerate in terms of attacks? Cyberattacks (as opposed to cyberespionage) have yet to create very high damages even when summed (perhaps under $100m a year). By contrast, conventional war is several orders of magnitude more expensive. What are the risks that by starting with a response to something that takes place only in cyberspace one ends up with something much more serious? Second, if we are talking about Russia, any response has to support NATO's overall posture with respect to that country; cyberspace cannot be considered in isolation.

In one of your numerous excellent papers, one particularly important sentence can be found. You wrote that "cyber operations can supplement war, but they cannot be the war". It is often forgotten that cyberattacks mostly enhance use of traditional tools (both military and political). Cyberspace can be utilised in a different ways, for instance the example of Ukraine conflict indicates that cyberspace can be used as an element of information warfare. Correct me if I am wrong, but it seems to me that the US underestimated this form of conflict in the past and focused rather on "hard" aspects of cybersecurity. Should it be changed in the future? How to deal with information warfare carried out in cyberspace?

In the 1990s, the concept of information war encompassed both psychological operations and hacking – despite vast differences between them. And whereas there are circumstances under which hacking can support psychological operations, they are limited circumstances. That said, both psychological operations and hacking may serve parallel strategic purposes, but that still needs to be worked out.

It is widely acclaimed fact that norms of behaviour can influence and shape global environment also when it comes to cyberspace. What are the most important aspects of particular countries' behaviour in cyberspace from the point of view of the US? Which international acts should be normalised in the first place?

The primary US goal is a norm that de-legitimises economically-motivated cyberespionage. A secondary US goal is a norm that forbids cyberattacks on critical infrastructure. The problem is less one of norms as such (after all, President Xi agreed to the first one), but agreement on how violations of such norms should be detected and acknowledged.

Presidential campaign in the US speeds up. Is cybersecurity an important element in candidates' programs? If yes, which aspects play crucial role?

Cybersecurity is playing a somewhat larger role in this year's Presidential campaign. Senator Webb mentioned it (Chinese cyberespionage, mostly) prominently in his remarks during the Democratic candidate debate, but no one followed up.
Some Republican candidates bring it up when arguing that the United States is coddling China. Once the Democrats and Republicans stop debating among themselves and debate each other, the issue may arise more strongly.

In September President Obama and Chinese President Xi Jinping announced a new cybersecurity agreement. Later on it was announced that the Chinese government arrested hackers at the request of the US government. What is the importance of the agreement, and can it be a real game changer when it comes to rather tense cyber US-Chinese

relations?

The agreement is significant for giving the United States a basis on which to threaten China if it continues economically-motivated cyberespionage (whereas, before, it would have been enforcing a norm that the Chinese never signed onto). However, as noted above, we have no norms for detecting and acknowledging norms violations. China has always denied cyberespionage whether of the sort that the United States deems illegitimate or of the sort that the United States itself, is accused of doing. As for the arrests, I would need to see more information.

Thank you very much for this inspiring interview. In the upcoming issues of the ECJ, we will elaborate on issues you pointed out. ■

Questions by:
dr Joanna Świątkowska