CENAA
Centrum pre európske a severoatlantické vzťahy

Policy Papers

CYBER SECURITY

AN INSIGHT TO CYBER WORLD WITH PROF. MICHAEL E.SMITH

by

Veronika Macková and Viktória Sučáková

As we kick of spring of 2014, GNC Team is starting quarterly insight to cyber world from the point of view of international cyber-security experts. Especially, in this interview, we examine cybersecurity from Professor Smith´s point of view. This series is particularly focused on European Union´s voluntary framewok, actions of whistleblowing and other important issues.

Q: What attracted you to the field of international security and security in general?

A: Security is the most fundamental problem in international relations, because if you don't have a secure environment in which human beings can operate, then they can't achieve any other goals. So for me it's kind of foundation of international relations. Information security in particular, obviously because of our reliance on information technology, now the back bone of global economy. If that aspect of global economy is threatened or undermined in some fashion, then I don't think we can achieve any other economic or social goals, so it's critical these days. But also having said that, we lack any coherent way to think about it. It's extremely important but also extremely underdeveloped as an conceptional area.

Q: What does Global Netizenship represents for you?

A: It's a research that doesn't mean anything to me yet. I know it exists out there in the world but as an academic I don't have a grasp of it yet. We are starting to work on that now. To how people act on the internet, how do they develop their identities, is a very under-theorized and under-researched area. That's why we're working on it at this university, to develop it.

Q: Are the governments around the world coping with the cybercrime, or are they just studying it?

A: I think a little of each but mostly trying to figure out what it is exactly. I had this problem when writing my textbook on international security. There is no consensus on what cybercrime is, or cyberbullying or cyberwarfare, all these different levels of engaging with the internet in negative fashion with no consensus on how to frame it as academic field. Governments are having the same problem and that's why they are dealing with it in a very fragmented and incoherent fashion. People in defense and war ministries do it in a certain way, and people in infrastructure do it different way, people in the criminal justice do it another way. So that's the part of the problem here.

Q: Does the European Union have the ability to fight against cybercrime?

A: It's already attempting to do that. The commission has its strategy against it. It's going to be very long term. But it's tied to the fact that the EU doesn't have a very good internet or information strategy in general. Even though it's trying to develop it. So the EU lacks some infrastructure projects that would really help facilitate actions against cybercrime, it lacks energy infrastructure, IT infrastructure, aerospace infrastructure, so it is all part of a larger pattern. The EU is failing to live up to its promise, yet it's attempting so we'll see.

Q: Do you agree with the statement that there is cyberwar out there?

A: Well, there are definitely thousands of attacks occurring on computers all over the world so if you frame that as a cyberwar then I would say yes but if you consider cyberwar as actions between governments, or government targeting another country then it's a lot more complicated.

Q: What about the 2010 Stuxnet?

A: If it is true that it was US and Israel who did this against Iran then you could consider it as a case of cyberwar. US is definitely developing some sort of defensive capability to prevent attacks from China or Russia. I definitely think that they are developing capabilities and plans of actions around the concept of cyberwar. US has a cybercommander now, so definitely US is institutionalized with it and once US starts to do something other countries start following whether it's good or bad.

Q: Why did you choose Mac by Apple, and how comfortable are you with it?

A: Mostly because Mac operating system is more stable. I've been using Windows for 20 years and it always had stability and security. I've had Mac for 4-5 years and these problems haven't occurred. It had never failed on me compared to Windows in the past. I've never used Linux so I can't compare it.

Q: Mr. Snowden's revelations about Prism have called into question the relationship between technology companies and governments. How you see this relationship?

A: I think it's much more complicated and secretive than the governments and companies like to admit. And also more likely to violate civil liberties in ways they want to keep it a secret and that's why Snowden is so important. I think he was right to reveal some of the information. The way US government has been dealing with this is very troubling in the case of Snowden but also in the cases of NSA doing all these programs so I think it's good that some of these materials have been released, not how it was done and all the other things around it but the general issue of the US government lying or keeping secrets about these programs was wrong. I think we'll see more of this. I think there will be more revelations to come.

Q: Who do you think created Stuxnet?

A: I don't know. I think it's believed it was US government.

Q: Do you believe US government could go that far?

A: Definitely. I think US government is capable of doing just about anything. If a government has a capability to do something, it will use it.

Q: Which countries in the Middle East would you consider as a base for the DDoS and why?

A: Israel, maybe because of the link with Iran, but also because of Israel's own capabilities and concerns. If other countries had capabilities, I'm not sure if they would use it in aggressive way, that is the question for me. US and Israel have ties, and the expertise that Israel has in technology and IT is clear.

Q: Do you think the recent events around NSA change people's perspective on governments and are people more aware of what is happening and do they care about it?

A: They are certainly more aware because of the revelations but I think they do care about their privacy but they are not willing to act on it. So they still give up information voluntarily to Facebook and other companies without thinking about the implications. Clearly they care about it but they don't care enough to protect it.

Q: How is the situation in US. Being from US, do you notice any reaction from your family, friends or colleagues?

A: I think most of Americans are still naïve about this situation. And they still trust the US government to do the right thing even if they might make mistakes along the way. That's why you have such a division in US about this controversy. You have half of the country thinking [Snowden] is the traitor and the other half thinking he is a hero. It shows you that the country is seriously divided in all these issues. Even if they don't like what the government did they still forgive the government because they think it's in their best interest. But there is another point of view, that the US will overstep its authority to protect itself in the way that will violate the civil laws and liberties.

Q: Over the past few years we have seen several actions of "whistleblowing" (WikiLeaks, Anonymous, Edward Snowden). At time it always seemed as they have made an impact on

the actions of governments. However, the more time passes nobody seems to talk about these issues anymore. Do you think people tend to forget and to what extent does these actions then have impact?

A: I think in the short term these actions have impact on governments and companies but in the long run they tend to fade away and governments, at least in the cases of US and UK, might talk about it briefly but there has been no serious reforms. At this moment we get to see a big crisis of privacy and internet security, but the reforms are very weak. As long as people are not seriously upset about this I don't think we'll see any change in the reforms. It will be up to individuals and firms to try to protect themselves.

Q: What is the future of cyber security within the field of IR?

A: In IR there is only very few people who are looking at it in IR theoretical conceptual perspective.

Q: What do you think is the reason?

A: Because it's very difficult to measure as a research question. There is no concept on how to even do that. I think it is a very promising topic within IR but it will take some time.

Q: How do you think should the international community deal with the question of cyber attacks?

A: There is the ideal way and the reality. Ideal way is that we'd have some sort of international agency that would be dedicated to these issues, like the IMF, WTO. But politically I don't think that's feasible. I think it will be done on an ad-hoc bases. And if US doesn't agree to something than it's very difficult to lead a cooperation. It is still a very decentralized approach for now but that might change if there will be some massive crisis that threatens wide range of actors, kind of like a disease. Then they might devote some agencies to it.
It is a cross national problem and it requires cross national operation and if you don't create an agency to deal with it on regular basis then you have to do it ad – hoc which I don't believe it's the appropriate way, but politically that's the way it has to be done right now.

Q: Do you think cyber terrorism is an adequate term for what Edward Snowden has done? Do you think it is appropriate to accept this as terrorism?

A: No, I don't think it's the appropriate term for this. The way I see terrorism is violence directed towards civilians because of reasons and I don't think he's done that.

Q: Obviously, internet is global and international. How does cyber security affect states on national level? Do you think it is a matter of nations (especially when it comes to USA) or does this case have to be dealt with globally and internationally?

A: I think again there are lots of parallels with pandemic disease, because disease has to be dealt with on national level but if you have a threat coming from outside then you have to have cooperation with the source. If it's coming from multiple directions then all the countries need to cooperate. But for diseases we have WHO, but for cyber attack what do we have? Interpol might try to help but it's still lacking behind a great deal. Some areas, like EU, are

making some progress. The EU is trying to have a regional approach. If this can work on regional level and EU can protect its member states then it will be helpful for the global system. It could be a model for other regions.

Q: Do you think this trend will continue, or are people scared after the last few cases.

A: I think it will continue, definitely.

Q: In your opinion, is there any justification for NSA to collect information on their citizens? Does this in any way affect democracy? And is this even democratic?

A: There is the government justification but that needs to be balanced with liberties and in US you have the freedom of speech, so I think these rights should be protected and if NSA wants to collect information it needs to have legal authority to do that. At the moment I think they've been using their capabilities to take up too much information. That needs to be scaled back.

Q: As most of life, social or political is currently dealt through computers. Do you believe that cyber security then becomes a focal point of security? Or is it possible that one day it might be the key aspect of international security?

A: I think it's becoming a focal point, theoretically it is possible. The more computers are used in traditional security issues, the more important cyber security becomes.

Professor M.E. Smith:

Professor Michael E. Smith joined the University of Aberdeen in 2010; prior to that he was a Reader in International Relations at the University of St Andrews and an Associate Professor of Political Science at Georgia State University in Atlanta. A native of western Pennsylvania in the US, he holds a PhD in Political Science from the University of California (Irvine) as well as an MA in International Affairs from The George Washington University. He has been a Fulbright scholar to the European Union in Brussels, a Council for European Studies fellow, a visiting research fellow at the Centre for European Policy Studies in Brussels, and a University of California Institute for Global Conflict and Cooperation/MacArthur Foundation fellow. He was the founder and first co-chair of the “EU as a Global Actor” interest section of the European Union Studies Association (2003-07), and he is on the editorial boards of the Journal of European Public Policy and European Security.

CENAA Policy Papers

No. 4/2014, Vol. 3

Centre for European and North Atlantic Affairs

Tolstého 9, 811 06 Bratislava

www. cenaa.org/publikacie/policy-papers/