GlobalResearch
Center for Research on Globalization

No Joke: US Think-Tank Suggests NATO Cyber-Attacks against Russia

Moscow Metro, St. Pete Power Grid, RT Offices

By Robert Bridge
Global Research, August 07, 2016
RT 5 August 2016

Region: Russia and FSU, USA
Theme: US NATO War Agenda

The hysterical 'information war' just stopped being funny. The influential Atlantic Council has released a paper calling for Poland to 'reserve the right' to attack Russian infrastructure, including Moscow's public transport and RT's offices, via electronic warfare.

There are some ideas that are so outlandish, so outrageous, so off-the-reservation weird that the only way they should enter the public realm is by sheer accident, or in haphazard fashion through whistleblowers and WikiLeaks data dumps.

Regrettably, however, that was not the case with the Atlantic Council's latest paper, alarmingly entitled 'Arming for Deterrence: How Poland and NATO Should Counter a Resurgent Russia'. The recommendations put forward in this paper are the result of a deliberate decision (predicated upon the unfounded idea that Russia would initiate a military attack against Eastern European and Baltic nations), and that's what makes its contents all the more disturbing.

Heeding Tolstoy's advice, let's jump right into the action: Page 12, paragraph 7 and I quote: "Poland should announce that it reserves the right to deploy offensive cyber operations (and not necessarily in response just to cyber attacks). The authorities could also suggest potential targets, which could include the Moscow metro, the St. Petersburg power network, and Russian state-run media outlets such as RT."

Holy hooliganism, Batman! That comment made me sit straight, spill my coffee and check to see if I wasn't perusing a parody piece by The Onion. No such luck. My gut reaction, however, was to ignore the bombast and hyperbole, since responding would only give the authors some satisfaction that they hit a nerve. And I must admit, they succeeded. In fact, they hit my sciatic nerve, the longest neuron transmitter in the human body that begins in the lower back and runs through the buttock and down the leg (I once underwent leg surgery and the doctor, in an experimental mood, I assume, injected anesthetics directly into this hot spot, which is about the equivalent of being hit by a dozen police Tasers at once).

In other words, ignoring this shocking remark was not an option. The reasons should be obvious. Though the paper 'merely' suggested "offensive cyber attacks," the Moscow Metro, which carries about 10 million commuters daily, has suffered a number of deadly attacks over the years. The last thing it really needs is an "offensive" attack of any kind.

On August 8, 2000, a bomb equivalent to two pounds of TNT detonated inside a pedestrian underpass at Pushkinskaya metro station in the center of Moscow. The attack claimed the lives of 12 and injured 150. On February 6, 2004, an explosion devastated a rush-hour carriage between the Avtozavodskaya and Paveletskaya stations, killing 41 and wounding over 100 commuters on their way to work. A marble plaque on the platform of the Avtozavodskaya Metro bears the names of the victims. On March 29, 2010, dual explosions 40 minutes apart hit the Lubyanka and Park Kultury stations during yet another morning rush hour, killing 40 and injuring 102 others.

Needless to say, Muscovites still carry a lot of emotional baggage from these tragic incidences, so for anybody to suggest the Moscow Metro (or any form of public transport, for that matter) come under some sort of attack is simply outrageous. Although an "offensive cyber attack" (isn't every attack by nature "offensive" – why the need to be tautological?) does not rank in the same category as a bomb attack, for example, it is nevertheless a form

of violence that could have catastrophic consequences.

Second, mentioning St. Petersburg (formerly Leningrad) – the site of a 872-day military siege by the Nazi Army (Sept. 1941 to January 1944) in which somewhere between 643,000 and 1.5 million civilians died of starvation, disease and bombardment – in the context of an attack is just stupid. Most likely it is a cheap effort by the authors to provoke an emotional response from the Russians, who take immense pride from the incomparable sacrifices made by the people of Leningrad (Perhaps even more disturbing, however, is the fact that there is a nuclear power plant 70 kilometers outside of St. Petersburg; would that fall under our author's purview for a cyber attack?). Why would the authors deliberately rile the Russians over one of their most culturally and historically significant cities? I have some wild guesses, but more on that a bit later.

Who needs Geneva's conventions?

I am a bit surprised that it is necessary to remind people – especially authors for an influential think-tank – as to what the Geneva Convention has to say with regards to protecting citizens. Article 51(2) of Additional Protocol I to the Geneva Conventions, explicitly states:

> "The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence, the primary purpose of which is to spread terror among the civilian population, are prohibited."

Although I am no lawyer, that statement seems pretty straightforward. Not only the act of violence, but "threats of violence"are prohibited, and an "offensive cyber attack" – which could be severely disruptive, even deadly, in our hyper-technological societies – would certainly qualify.

The authors of the Atlantic Council piece, therefore, are skirting the margins of legality, not to mention sanity, I would say, especially when we consider that Russia has not demonstrated hostile intentions against any Eastern European country, except for those invasions that exist in the vivid imaginations of NATO planners.

Now, concerning the other "potential targets" that our ambitious authors have lined up for Poland's punchy army, namely, "Russian state-run media outlets such as RT," once again the authors have gone off the rails as far as the law is concerned. That is because media facilities are considered to be civilian installations and strictly off-limits to any sort of attack, "offensive cyber attacks" included.

"Radio and television facilities are civilian objects and as such enjoy general protection. The prohibition on attacking civilian objects has been firmly established in international humanitarian law since the beginning of the twentieth century and was reaffirmed in the 1977 Protocol I and in the Statute of the International Criminal Court," advises Marco Sassoli, Antoine Bouvier and Anne Quintin in a case study regarding the protection of journalists.

There is yet another problem with this particular paper that became apparent just days after its publication. First, let us reconsider the gratuitous advice the authors have for the Polish authorities (who will hopefully take a pass on this think-tank junk): "Poland should announce that it reserves the right to deploy offensive cyber operations (and not necessarily in

response just to cyber attacks).” That parenthetical comment at the end is not my addition; it appears in the original. So what exactly would qualify Russia’s civilian infrastructure for being on the receiving end of some sort of Polish attack via electronic warfare? The authors do not tell us. I guess they just want to keep everybody in the dark, so to speak.

In any case, the comment is problematic and could have serious unforeseen consequences at least as far as already strained Russian-Polish relations go. After all, there always remains the risk that there will be, in some theoretical future, an “offensive cyber attack” of unknown origin on the Moscow Metro, St. Petersburg power grid or at RT offices.

Needless to say, such an unexpected turn of events would not look very good for the Polish authorities – even if they are innocent of such an aggression. It would look much worse, of course, should an “offensive cyber attack” result in injury or death to any citizens in Russia (It needs emphasized at this point that the possibility exists of some third-party deliberately initiating a cyber attack in the hope of aggravating tensions between Russia and Poland, which would give NATO the justification it desperately needs for its dwindling relevance in a post-Cold War world).

Under a section entitled “Policy declarations”, the authors give the Polish authorities another misguided suggestion: “Poland should make clear policy declarations regarding its behavior in the event of Russian incursions and on targeting within Russia.” The last part of that sentence is unclear and could be interpreted as two distinct events: 1. “The event of Russian incursions”, and 2. “Targeting within Russia” – bereft of any initial Russian incursion.

Meanwhile, the term “offensive cyber attacks” appears in another section of the paper where the authors remark: “NATO has tied its own hands by declaring that it would not use all tools available to it, such as refraining from using offensive cyber operations. Holding back from offensive cyber operations is tantamount to removing kinetic options from a battlefield commander.” Using and comparing these two terms in the same sentence is troubling. As Timothy Noah wrote in Slate, kinetic means“dropping bombs and shooting bullets—you know, killing people.”

Ironically, just days after this nonsense burst asunder from the busy bowels of US

'thinktankdom', the Russian Security Service (FSB) reported that computer networks of some 20 Russian state, defense, scientific and other high-profile organizations were infected with malware used for cyber-espionage, describing it as a professionally coordinated operation.

"The IT assets of government offices, scientific and military organizations, defense companies and other parts of the nation's crucial infrastructure were infected," the FSB said in a statement as cited by the Russian media.

Although these sort of attacks will continue to occur in our hi-tech societies, it seems a bit reckless to suggest that one state should say it "reserves the right" to initiate "offensive cyber attacks" against civilian targets, especially when the country under consideration, Russia, has not demonstrated any hostile intentions towards its neighbors. But that is certainly not the impression the reader will get from perusing the aggressive Atlantic Council report, which paints a totally misleading picture of Russia.

Who writes this stuff?

The disturbing advice put forward in this paper is more understandable when we know the background of the authors.

Gen. Sir Richard Shirreff, NATO's Deputy Supreme Allied Commander Europe from 2011 to 2014, is now partner at Strategia Worldwide Ltd. He recently published "2017: War with Russia", the plot of which is pretty much self-explanatory.

It is hard to top the late fiction writer Tom Clancy when it comes to presenting (Soviet) Russia as the world's preeminent villain, but Shirreff certainly gives the author of "The Hunt for Red October" a run for his money.

NATO, according to Shirreff, will be at war with Russia by May 2017 (Surprise – just in time for the one-year anniversary of Shirreff's Russophobic thriller. Oh, happy sales!). Russian forces will invade the Baltic States and threaten to employ nuclear weapons if NATO attempts a military response. "A hesitant NATO will face catastrophe… the day of reckoning for its failure to match strong political statements with strong military forces finally arrives," his trembling fingers typed.

Amazing what a democratic referendum by the good people of Crimea to join the Russian Federation can do to some people's overactive imaginations.

Sadly, the primary motivator for such attacks on Russia boils down to the most primal motivator of them all: the profit motive. As a partner at Strategia Worldwide Ltd, which provides clients with "a comprehensive approach to corporate risk management… in complex, dangerous and difficult environments," according to its sleek website, Shirreff's groundless predictions about Russian aggression against its neighbors will probably draw more customers through Strategia's front door. Or boost book sales. Either way, it doesn't bode well for EU-Russian relations when rabble-rousers can get away with hawking phantom fears and libelous lies for filthy lucre.

But this non-fiction tale just gets more fantastic. The other author, Maciej Olex-Szczytowski, is described as an "independent business adviser, specializing in defense." In 2011-12 he was Special Economic Adviser to Poland's Foreign Minister, Radoslaw Sikorski.

But the biography missed the really juicy part of Olex-Szczytowski's resume.

"Maciej Olex-Szczytowski is Adviser on Poland to BAE Systems, Europe's largest company in the Defence Sector. A commercial and investment banker by training, he has led some €50 billion worth of transactions in Central Europe, and has provided advice to numerous corporations and governmental entities in the region."

Well now the warmongering jibes against Russia is starting to make some sense, at least from a business portfolio perspective.

Imagine. We have a former general turned business executive who is predicting that Russia will – for some inexplicable reason – invade the Baltic States (I can only presume for its excellent pastries and liquors) in 2017, teaming up with an investment banker who oversees the sale of tens of billions of dollars in military hardware to the EU, now advising Poland to "reserve the right" to launch an "offensive cyber attack" against Russian civilian infrastructure.

No conflict of business interests there, right? Nah! It is individuals like these, for whom the entire planet is one big business opportunity, and to hell with the risk of accidentally kick-starting a beast called Armageddon, who are the real regional aggressors.

Hopefully the Polish authorities are wise enough to see through this thinly veiled and very revolting business plan and politely reject the self-interested suggestions of Richard Shirreff and Maciej Olex-Szczytowski. With friends like these two, who needs enemies? After all, it will be Poland that will be forced to pay the piper the price of ruined relations with Russia, not the European military industrial complex, which will only reap a windfall should it come

to fruition.

Articles by: Robert Bridge