GlobalResearch
Center for Research on Globalization

War Games in Cyberspace: NATO's Cyber Defense Exercises Coincide with "Anonymous" Cyber Attacks against Ukraine

NATO Cyber Defense Center in Tallinn, Estonia features a fusion of modern technology with outdated cold war ideology

By Peter Adams
Global Research, December 26, 2013

Region: Europe, Russia and FSU
Theme: Militarization and WMD, US NATO War Agenda

Barely acknowledged by the mainstream media, NATO launched in late November its largest-ever cyber defense exercises "Cyber Coalition 2013" to test the Alliance ability to defend its networks from attacks.

The exercises involved some 500 experts – more than 100 participants from the NATO Cyber Defense Center for Excellence and over 300 cyber defense experts from 32 states-members and partners of the Alliance, who worked remotely.

Cyber Coalition 2013 continued the line of NATO exercises Steadfast Jazz 2013, which were held in Poland and the Baltic states in the beginning of November.

Coincidence?

Besides repulsion of aggression against Estonia from an imaginary state Botnia, the exercises also featured testing NATO cyber defense mechanisms. By an amazing coincidence, in the very beginning of the exercises a number of Ukrainian, Russian, Polish and Baltic state sites underwent an attack . Even the site of NATO Cyber Defense Center in Tallinn was down for some hours.

OBSCURE GUESSWORK.

It's not still clear who was behind the attack, though there were some reports of a notorious hacker group Anonymous Ukraine, who cracked some NATO servers in 2011, claiming responsibility for it.

The day before the attack Anonymous Ukraine published a video to announce the beginning of the "Independence" operation against both Russian and European options for Ukraine integration. Up to here everything seems quite clear. However, it's strange that after the Estonian authorities lost control of the Ministry of Defense site for almost 24 hours (!), they decided not to conduct an investigation of the incident under the pretext of major expenses necessary. Quiet a strange statement to come from a country which hosts NATO Cyber Defense Center, which was created to defend Estonia against cyber attacks.

In Ukraine, things were different. The hacked sites of Ukrainian government bodies (the Prosecutor General, SBU medical service, etc.) featured a banner of NATO Cyber Defense

Center in Tallinn warning that the sites didn't correspond to NATO security standards. Despite the hype in the social networks, there was no official reaction to the incident. Obviously, Kiev decided to swallow that to avoid "unnecessary consequences".

It's clear that Yanoukovich didn't have enough guts to accuse NATO of cyber terrorism or conduct an independent investigation. By the way, while some Polish, Latvian and Estonian sites were also attacked, only Anonymous Ukraine managed to give an appropriate reaction.

Brussels, naturally, denied any involvement in the incidents. In the midst of the exercises NATO Cyber Defense Center in Tallinn officially announced that someone just used its name to discredit the work of the alliance. However, the perpetrator was never named (https://www.ccdcoe.org/453.html).

What is not possible for the official bodies becomes real with the help of the expert community, namely, the International Center for defense studies in Tallinn (again) under the direction of a notorious informational provocations specialist, a retired U.S. diplomat and political scientist Matthew Bryza. Piret Pernik, an expert of the Center, made a thorough chronological research of the Steadfast Jazz 2013 incidents only to come to a staggering conclusion: the trace goes to Russia.

On the one hand, it's quite clear that from the Estonian point of view Russia is the only possible perpetrator. On the other hand, there should be at least some evidences. Pernik is sure that she has it.

In her opinion, the basic evidence is that Russian journalists reporting on this unfortunate incident dared to came with a hypothesis of what happened. Since Pernik is sure that Russia media are controlled by the FSB, their hypothesis is, evidently, a product of the Russian special services, which were certainly involved in the hack. A wonderful example of impeccable logic.

In fact, Russian media only proposed the evident – the attack was deliberately or non-deliberately executed by NATO in the course of the Steadfast Jazz 2013 exercises which tested the Alliance cyber defense capabilities. This conclusion becomes obvious after viewing the hacked sites, which displayed a banner claiming that the resource didn't correspond to NATO cyber security standards. The banner also included the logo of NATO Cyber Defense Center in Tallinn and telephone numbers of the contact persons.

Also, possessing some internet search skills proves to be enough to check that the "FSB-controlled" Russian media reports were, in fact, secondary information, since they provided only a digest of the wide discussion on blogs and forums.

Pernik also believes that the attack on Ukrainian and NATO sites was carried out from a Georgian IP-address. In her opinion, it provides yet another evidence of Russian trace. Well, firstly, what a Georgian IP has to do with Russia? Secondly, there was no investigation. That's why Pernik cites an anonymous cyber expert, and it sounds as ridiculous as "FSB-controlled Russian media". There was no explanation of the origin of the IP and it's not clear why the IP is mentioned by an independent expert, while the NATO Center remains silent.

A HUMILATING REPROACH FOR TALLINN

As it happens, some Ukrainian experts we contacted on conditions of anonymity are absolutely sure, that the sites of the Ukrainian Prosecutor General and SBU were attacked

from an Estonian IP-address. The experts say that this is why the Ukrainian authorities had to keep silence. Naturally, Kiev saw the attack as a warning send by NATO Cyber Center to its state-partners to inform them about the vulnerability of their internet resources.

Pernik also tries to prove Russian involvement by saying that the incidents got a wide coverage only in Russian media. That's just not true, and anyone can check it after a bit of googling. It is hard to miss a publication of Jane's Defence magazine, which points out that the incident is a humiliations for a country which started to receive huge financial support to develop cyber security after a serious cyber attack in 2007.

It should be noted that Tallinn was chosen as the NATO Cyber Defense Center HQ due to Estonian pressing requests to ensure its cyber security, caused by an outspread of computer attacks after the popular protest followed the dismantling of a Soviet Soldier monument in 2007. At that time, Estonian government also blamed Russia and demanded NATO to defend the country against the cyber attacks.

So, who is the real culprit behind the attacks on Ukrainian, Russian and Baltic sites in November? The cyber security experts agree that it is very difficult to investigate the activities of hacker groups and individuals. Cyber wars are becoming increasingly sophisticated, and it's almost impossible to check, confirm or disprove the information on the internet. That's why the state special services are collaborating with hackers or acting on their part.

Thanks to Edward Snowden the world is now aware of the illegal actions of the American special services, including computer piracy, stealing of personal information and hacking foreign state and private informational resources. As a matter of fact, the U.S. Cyber Command and NSA don't care about keeping their work secret anymore – it's enough to remember the speech delivered by Keith Alexander in Florida in the summer of 2013.

A SPUR TO HACKERS

As mentioned above, the cyber incidents got a wide coverage in the Ukrainian social networks and specialized hacker forums. The popular opinion is that Anonymous Ukraine is a pseudonym for some special service, probably even NSA or NATO Cyber Security Center itself. It is also believed that the cyber attacks were in fact carried out as training for NATO Center experts in the course of the Steadfast Jazz 2013 exercises, which aimed at testing the methods on "dummies", who could not provide an adequate response.

Another version states that the attack that involved NATO Cyber Center could have happen due to a computer mistake. Finally, it may well be that NATO cyber security experts executed a prepared scenario in cooperation with their counterparts from Latvia, Lithuania, Poland, Ukraine and Estonia.

It is likely that we would never know who was behind these attacks – Ukrainian hackers, NATO cyber security experts or someone else. However, there is a general impression of a wide-scoped and sophistically planned provocation, carried out by two centers in Estonia in order to display Russia as an insidious cyber aggressor, draw some attention to its activity and provide a reason for increasing NATO cyber security budget.

Meanwhile, Russia is still behind the U.S. and other NATO members in the sphere of cyber security. The announced formation of cyber units is still to happen and there is no news

about cyber security exercises.

It is not a coincidence that Russia promoted an UN initiative of limitation of the arms race in the informational sphere and offered other countries to join the Convention of International Informational Security.

While the U.S. and NATO are paying great attention to cyber warfare and refusing to treat other countries as equals, they, in fact, only encourage the interest of terrorist organization in asymmetric response and spur hackers all over the world. On that background, Tallinn centers blaming Russia seems as a failed attempt of shifting responsibility for strategic errors, technological mistakes and wrong choice of partners. As for the eloquence of the Estonian analysts, it is probably explained by an uneasy conscience, which, as it is known, betrays itself.

Peter Adams <freelance5media@gmail.com>

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Peter Adams