GlobalResearch
Center for Research on Globalization

Police State North America: The U.S.-Canada Integrated Cybersecurity Agenda

By Dana Gabriel
Global Research, November 13, 2012
Be Your Own Leader

Region: Canada, USA
Theme: Police State & Civil Rights

As part of the Beyond the Border initiative, the U.S. and Canada are strengthening cybersecurity cooperation. In a move that received little attention, both countries recently announced a joint cybersecurity action plan. Cyber threats know no national borders which has made the issue an important security concern. A fully integrated North American security perimeter would be entrusted with preventing and responding to any such attacks.

One of the key priorities identified in the November 2011 Beyond the Border Action Plan is cybersecurity. The agreement lays the framework for enhancing U.S.-Canada, "bilateral cyber-security cooperation to better protect vital government and critical digital infrastructure and increase both countries' ability to respond jointly and effectively to cyber incidents. This will be achieved through joint projects and operational efforts, including joint briefings with the private sector and other stakeholders, and the enhancement of real-time information sharing between operation centres." The deal will also works towards strengthening, "cooperation on international cyber-security and Internet governance issues to promote prosperity, enhance security and preserve openness in our networked world." Merging cyber threat strategies would force Canada to further bring its security practices in line with American ones and under the reach of the Department of Homeland Security (DHS).

On October 26, Public Safety Canada and the DHS released a Cybersecurity Action Plan which represents a key commitment under the Beyond the Border agreement. A press release explained that the specific goals include, "enhancing collaboration on cyber incident management between each country's cyber security operations centres, improving information sharing and engagement with the private sector, and continuing the ongoing collaboration between Canada and the U.S. on the promotion of cyber security awareness to the public." The new joint action plan promotes a shared approach to cybersecurity and digital critical infrastructure protection. Building on these initiatives, both countries also seek to further integrate cyber capabilities into military command structures.

Earlier this year, Defense Secretary Leon Panetta authorized the creation of the Joint Cyber Center (JCC) run by the North American Aerospace Defense Command (NORAD) and U.S. Northern Command. The JCC will bring together personnel from the intelligence, operations and command control systems divisions. The aim is, "To better integrate cyber into the headquarters missions by improving situational awareness in the cyber domain, improving the defense of the commands' networks and providing cyber consequence response and recovery support to civil authorities." In June, DefenseNews reported that Secretary Panetta, "approved a new organizational framework, a plan designed as a 'first step' towards

standardized cyber operations." This includes having a JCC at each geographic combatant command which is part of ongoing efforts to not only boost U.S., but continental cyber defense capabilities. In the near future, the U.S. and Canada could create a binational "cyber-NORAD" to protect North America from shared threats.

The North Atlantic Treaty Organization (NATO) released an updated Policy on Cyber Defence in June 2011. According to NATO's website, "This revised policy offers a coordinated approach to cyber defence across the Alliance with a focus on preventing cyber attacks and building resilience." It will act as the framework, "for how NATO will assist Allies, upon request, in their own cyber defence efforts, with the aim to optimise information sharing and situational awareness, collaboration and secure interoperability." The new policy also, "sets the principles on NATO's cyber defence cooperation with partner countries, international organisations, the private sector and academia." In May of this year, the Chicago Summit Declaration, "committed to provide the resources and complete the necessary reforms to bring all NATO bodies under centralised cyber protection." It also pledged to, "further integrate cyber defence measures into Alliance structures and procedures." U.S.-Canadian military cooperation also extends through NATO and this includes in the realm of cybersecurity.

There are reports that President Barack Obama may be close to issuing a cybersecurity executive order as a means of bypassing Congress. Under the guise of cybersecurity, the U.S. and Canada have been individually pushing draconian legislation domestically which would grant government agencies sweeping new powers. The implications would be far reaching and pose a risk to privacy and civil liberties. Through the Beyond the Border initiative both countries are pursuing an integrated cybersecurity agenda. As they move forward and address common threats to North America, cyber and perimeter security will be further defined and dominated by U.S. interests.

Dana Gabriel *is an activist and independent researcher. He writes about trade, globalization, sovereignty, security, as well as other issues. Contact: beyourownleader@hotmail.com. Visit his blog at Be Your Own Leader*
