US Wages Cyberwar Abroad Under Cover of "Activism"

By Joseph Thomas

Global Research, August 29, 2017
New Eastern Outlook

Region: Asia, USA
Theme: Intelligence, Police State & Civil Rights, Terrorism, US NATO War Agenda

The threat of cyberterrorism has competed for centre stage in American politics with fears of "Russian hackers" disrupting everything from elections to electrical grids. And yet as US policymakers wield threats of cyberterrorism to promote a long and growing list of countermeasures and pretexts for expanding its conflict with Moscow, it is simultaneously promoting very real cyberterrorism globally.

Worst of all, it does so under the guise of "activism."

The Carnegie Endowment for International Peace recently published a paper titled, "Growing Cyber Activism in Thailand."

In it, readers may have expected a detailed description of how independent local activists were using information technology to inform the public, communicate with policymakers and organise themselves more efficiently.

Instead, readers would find a list of US-funded fronts posing as "nongovernmental organisations" (NGOs) engaged in subversion, including attacks carried out against Thai government websites aimed at crippling them, the dumping of private information of ordinary citizens online and coercing policymakers into adopting their foreign-funded and directed agenda.

US-Backed Cyberterrorism

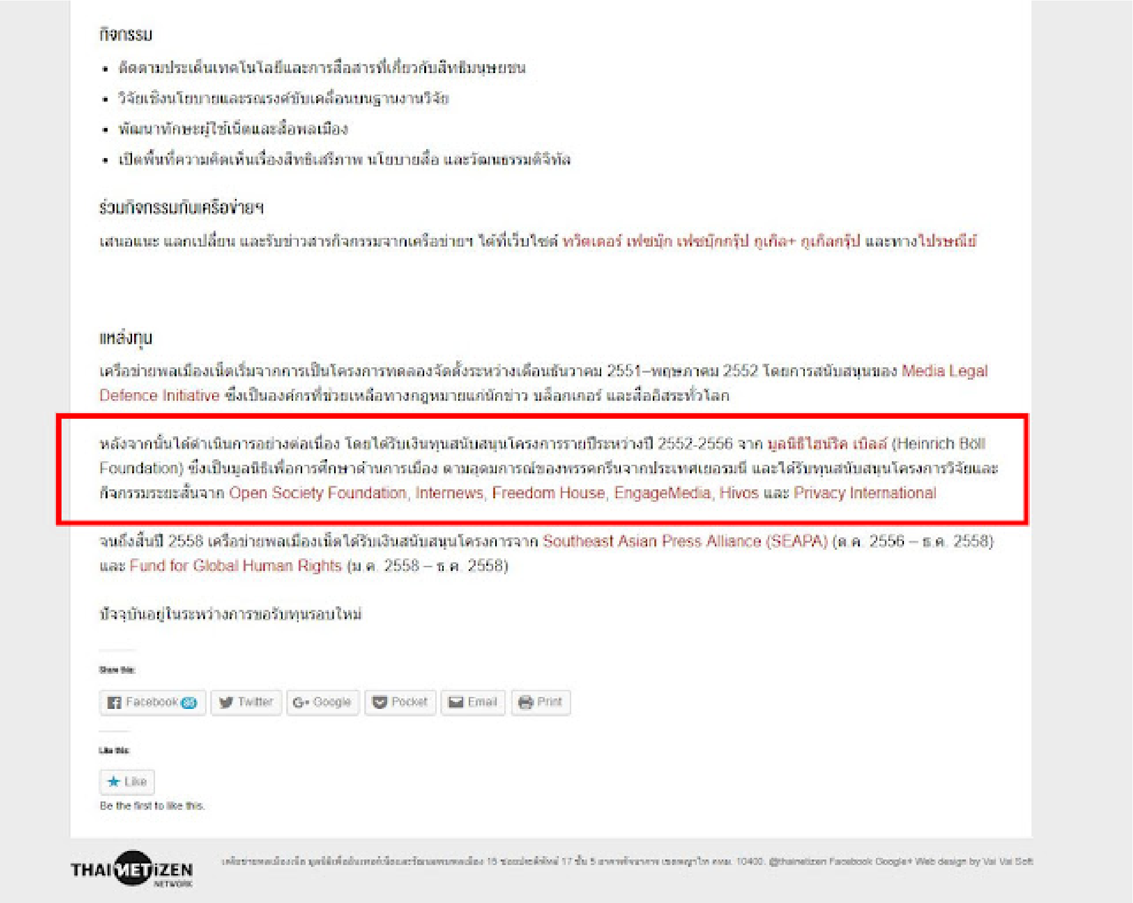
The paper cites petitions created by the US-funded Thai Netizen Network on the US-based petition site, Change.org as well as distributed denial of service attacks (DDoS) aimed at crippling essential government websites, a campaign defended by US-funded Thai Netizen as being *"virtual civil disobedience."*

The paper would claim (our emphasis):

> The most innovative countermeasure was a series of Distributed Denial of Service (DDoS) attacks: an anonymous group, Thailand F5 Cyber Army, declared a cyberwar on the Thai government by encouraging netizens to visit listed official websites and continuously press F5 on their keyboards to refresh the pages. **The goal was to overwhelm web servers and cause a temporary collapse of the websites of the Ministry of Defense, Ministry of Information and Communication Technology, Government House of Thailand, National Legislative Assembly, and Internal Security Operations Command.** The group disseminated detailed instructions on the operation to its anonymous activists. It then demanded that

> the junta cancel its Single Gateway proposal.
>
> Most of the attacks were successful. Activists wanted to demonstrate the government’s technological ineptitude and its lack of capacity to manage the Single Gateway. **Arthit Suriyawongkul, coordinator of the Thai Netizen Network, described the campaign as virtual civil disobedience—an online version of the nonviolent resistance practiced by civil rights groups in the United States.**
>
> In another case, an activist group called Anonymous launched a #BoycottThailand campaign on Twitter **and reportedly hacked government websites, snatched confidential information from official databases, and shared it online.**

The Thai Netizen Network is funded by the US State Department via the National Endowment for Democracy (NED) subsidiary, Freedom House, Open Society and a number of other foreign governments and corporate-funded foundations.



กิจกรรม

- ติดตามประเด็นเทคโนโลยีและการสื่อสารที่เกี่ยวกับสิทธิมนุษยชน
- วิจัยเชิงนโยบายและรณรงค์ขับเคลื่อนบนฐานงานวิจัย
- พัฒนาทักษะผู้ใช้เน็ตและสื่อพลเมือง
- เปิดพื้นที่ความคิดเห็นเรื่องสิทธิเสรีภาพ นโยบายสื่อ และวัฒนธรรมดิจิทัล

ร่วมกิจกรรมกับเครือข่ายฯ

เสนอแนะ แลกเปลี่ยน และรับข่าวสารกิจกรรมจากเครือข่ายฯ ได้ที่เว็บไซต์ ทวิตเตอร์ เฟซบุ๊ก เฟซบุ๊กกรุ๊ป กูเกิล+ กูเกิลกรุ๊ป และทางไปรษณีย์

แหล่งทุน

เครือข่ายพลเมืองเน็ตเริ่มจากการเป็นโครงการทดลองจัดตั้งระหว่างเดือนธันวาคม 2551–พฤษภาคม 2552 โดยการสนับสนุนของ Media Legal Defence Initiative ซึ่งเป็นองค์กรที่ช่วยเหลือทางกฎหมายแก่นักข่าว บล็อกเกอร์ และสื่ออิสระทั่วโลก

หลังจากนั้นได้ดำเนินการอย่างต่อเนื่อง โดยได้รับเงินทุนสนับสนุนโครงการรายปีระหว่างปี 2552-2556 จาก มูลนิธิไฮน์ริค เบิลล์ (Heinrich Böll Foundation) ซึ่งเป็นมูลนิธิเพื่อการศึกษาด้านการเมือง ตามอุดมการณ์ของพรรคกรีนจากประเทศเยอรมนี และได้รับทุนสนับสนุนโครงการวิจัยและกิจกรรมระยะสั้นจาก Open Society Foundation, Internews, Freedom House, EngageMedia, Hivos และ Privacy International

จนถึงสิ้นปี 2558 เครือข่ายพลเมืองเน็ตได้รับเงินสนับสนุนโครงการจาก Southeast Asian Press Alliance (SEAPA) (ต.ค. 2556 – ธ.ค. 2558) และ Fund for Global Human Rights (ม.ค. 2558 – ธ.ค. 2558)

ปัจจุบันอยู่ในระหว่างการขอรับทุนรอบใหม่

เครือข่ายพลเมืองเน็ต มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง 15 ซอยประดิพัทธ์ 17 ชั้น 5 อาคารพี่จาหลาน เขตพญาไท กทม. 10400. @thainetizen Facebook Google+ Web design by Vai Vai Soft

The role of a foreign-funded front coordinating efforts to undermine Thailand’s national security, including promoting cyberterrorism as “civil disobedience,” carries with it many implications. That the US is the foreign state promoting these activities in Thailand, undermines its own efforts to define and combat cyberterrorism back home.

What is Cyberterrorism?

Cyberterrorism is described on the United States Federal Bureau of Investigation’s (FBI) website as:

> …the use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population.

Attacking government websites millions of people across Thailand depend on for information and services while pilfering the personal information of thousands of ordinary citizens clearly fits the definition of not only cyberterrorism because of the political motivations involved, but also malicious criminality in general.

Unlike alleged Russian hacks which divulged emails detailing impropriety among American politicians, the information pilfered by US-backed hackers in Thailand included the personal information of millions of ordinary citizens using government services as part of their daily lives.

Bangkok Post would fill in the missing information intentionally omitted from the Carnegie Endowment paper, reporting that:

> Files posted by Anonymous and examined by the Bangkok Post appear to be from the court system, as the Anonymous posters claimed.
>
> An SQL database file of 1.1 gigabytes contains thousands of names, ID card numbers, photos, email addresses, personal phone numbers and more — all in clear text.

By dumping this information online, US-backed hackers targeted ordinary citizens, jeopardising their privacy and exposing them to criminal elements the world over involved in identity theft.

US Cyberterrorism is not "Activism"

The Carnegie Endowment paper itself was drafted by **Janjira Sombatpoonsiri**, assistant professor of political science at Thammasat University, Thailand. She is also cited as a member of the Carnegie Endowment's Civic Activism Network. Not only is she an active, contributing member of Thailand's foreign-backed opposition, she is admittedly involved in a foreign think-tank funded by foreign corporate interests.

The Carnegie Endowment includes among its sponsors in its 2016 annual report; the US government, pharmaceutical giants including Gilead, petrochemical monopolies including Chevron, British Petroleum and Shell, defence contractors including Lockheed Martin and several automakers including Ford.

US-funded Thai Netizen participates in a likewise foreign funded Amnesty International protest. Thai Netizen and the agenda is promotes is neither Thai nor activism. It is foreign interference, and now, constitutes aiding and abetting cyberterrorism.

Like many other episodes of extraterritorial political interference up to and including military intervention, America's meddling in Thailand is done on behalf of corporate interests seeking to expand their respective and collective hegemony both regionally in Asia vis-a-vis Beijing, and globally. This interference is done under the cover of rights advocacy, both by the think tanks and foundations funding it and those in Thailand receiving foreign cash.

The US use of cyberterrorism in Thailand and beyond should come as no surprise. It augments already ongoing efforts by US-backed opposition in Thailand to destabilise and upend Thailand's political order which has included armed terrorism.

Most recently, a string of bombings plagued Bangkok, including one targeting a hospital. At various junctures during Thailand's political conflict, foreign-backed opposition has brought militants into the streets. In 2010, nearly 100 would die over the course of several weeks, culminating in citywide arson leaving areas of Thailand's capital, Bangkok, resembling a war zone.

To see US-sponsored authors attempting to promote cyberterrorism as "activism" in Thailand also comes as no surprise. When Thailand's opposition carries out armed terrorism, US-sponsored media and policy think tanks often attempt to spin it as well. Other forms of more traditional subversion are also regularly defended by the US and its myriad fronts posing as rights advocates as "activism."

Understanding that it is not "activism," but by America's own very definition, cyberterrorism, helps disarm this malicious campaign posing as "civil disobedience" and "activism," and allows nations like Thailand to defend themselves through enhanced technological security measure as well as legislation.

***Joseph Thomas** is chief editor of Thailand-based geopolitical journal, The New Atlas and contributor to the online magazine "New Eastern Outlook".*

All images in this article are from the author.

The original source of this article is New Eastern Outlook

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **Joseph Thomas**

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

For media inquiries: publications@globalresearch.ca