We Have an Antiquated Framework

Candace Yu is an associate security fellow with the Truman National Security Project. She was a cyberpolicy adviser at the U.S. Department of Defense from 2010 to 2012.

Updated February 28, 2013, 6:38 PM

We need new rules of engagement in cyberconflict. And they must be flexible enough to allow the military to conduct specific — yet limited — cyber-operations without presidential authorization. Requiring the president to approve all cyber offensive operations is an antiquated framework that made sense when cyberthreats were less sophisticated. Times have changed.

> Prescribed thresholds for action, along with flexibility to act, will increase the military's ability to respond appropriately.

What we need are prescribed thresholds for action. This, along with flexibility to act, will increase the military's ability to respond appropriately and proportionally to cyberattacks. These thresholds will ensure proportionality in offensive actions and compliance with customary international humanitarian law.

This measured framework is necessary, because attributing who launched cyber-attacks is complicated. Today, the military might know where a cyberbreach originated, but it cannot discern key factors: Who sat at the keyboard? Who financed the attack? Is the culprit and financier a state or nonstate actor? Why did they attack? These answers are critical to inform policymakers and determine what constitutes a "cyber" act of war.

Some have called for authorizing the military to defend private corporate networks and critical infrastructure sectors, like gas pipelines and water systems. This is unrealistic. The military has neither the specialized expertise nor the capacity to do this; it needs to address only the most urgent threats. These calls also disregard privacy concerns about military involvement in private networks. As a result, everyone has a role to play in cybersecurity, and the military should get involved only in extreme circumstances as defined by the prescribed thresholds.

No one expects the military to act every time Facebook's networks get hacked. And no one expects the military to serve as Facebook's primary security provider. But, if a cyber-intrusion creates a large-scale power loss in the dead of winter, we should explore military options. Many lives may depend on it.

Join Room for Debate on Facebook and follow updates on twitter.com/roomfordebate.

Topics: Internet, cyber warfare, cybersecurity

8 Comments

Share your thoughts.

JHL Washington, DC

@Bosco Ho - I think there's is ample room for cybersecurity response in an accountable and appropriate manner without needing presidential authorization every time the government responds to the hacking of an email or phishing attempt. Having a standard procedures for "limited" operations (the part of the quote you left out) doesn't have to devolve into a military run-amok or schemes of deniability. Opportunities for abuse? sure. but that's an ever-present risk for all command structures where power is delegated.

March 1, 2013 at 12:25 p.m. RECOMMENDED 1

Bosco Ho Boston, MA

@JHL and @verkouille:

Perhaps I read Ms Yu wrong but I don't think she meant per incident. Sure, the president should not be a micro manager. You need an approval to buy some pencils or even laptops

However, President Obama, or any president following him to the White House for that matter, needs to know if there is A) a need to respond to a cyber threat worthy of a Pentagon, NSA, CIA and/or FBI's attention and B) especially if it goes beyond a defensive posture

To digress a little, while I know nothing about cyber defense, I'd imagine you can in A) a pure defensive mode like firewall erection or virus detection and eradication or B) counteroffensive mode like setting up honeypots etc

READ MORE COMMENTS