Former NATO Commander: Alliance Needs to Take Cyber Fight to Russia’s Door

- By Patrick Tucker Read bio ▸

July 6, 2017

Topics

- NATO

AP / Virginia Mayo

AA Font size + Print

Supreme Allied Commander Europe U.S. Air Force Gen. Phillip Breedlove speaks during a media briefing at NATO headquarters in Brussels on Thursday, Feb. 11, 2016.

- F≡cebook
- Twi??e!
- LinkedIn
- ▸ m≡il ?his ≡!?icle

- By Patrick Tucker Read bio ▸

July 6, 2017

In May, a former NATO supreme commander urged the alliance to plan an offensive cyber policy to combat Russian information influence operations.

Philip Breedlove was getting hacked by the Russians before it was cool. In 2016, the same group that penetrated the Democratic National Committee also stole the former supreme commander of NATO's personal emails, and published them to a Kremlin-produced website called DC Leaks. Recently the Air Force general advocated for a strong alliance pushback on Russian cyber-influence operations.

He says it must start with a strong NATO policy that would allow the alliance to conduct offensive cyber and information operations against Russia. His views contrast with those of President Donald Trump who, on the eve of his first meeting with Vladimir Putin, again refused to acknowledge the extent of the Kremlin's actions aimed at the U.S. election and declined to voice support for tough measures.

Speaking at a May security forum, Breedlove said that it was up to the U.S. and NATO to hold Russia accountable for its actions, and that accountability should take the form of offensive cyber and information attacks. "We in NATO have incredible cyber capability. But we in NATO do not have an incredible cyber policy. In fact, our policy is quite limiting. It really does not allow us to consider offensive operatives as an alliance in cyber," he said.

One of the tenets of the NATO alliance is that a military attack on one member triggers the collective-defense provision dubbed Article 5. But alliance leaders are still trying to figure out when a network attack might constitute an act of war. In June 2016, NATO Secretary General Jens Stoltenberg told reporters that a cyber attack on an ally could trigger an Article 5 response. But he said that the threshold would have to be very different than it is for a bombing, firefight, or some other violent, physical act of war. "It's hard to imagine a conflict without a cyber dimension. So, yes, cyber can trigger Article 5, but the same time I think it's also important to understand that cyber is not something that always triggers Article 5," he said.

A month after Stoltenberg spoke, NATO nations signed a Cyber Defense Pledge to increase collective funding for cyber deterrence and training and to seek industry partnerships. NATO nations also stepped up their cyber exercises. The largest one so far April's Locked Shields took place in Estonia and featured 800 participants from 25 nations and more than 2,500 simulated cyber attacks.

Neither the secretary general's words nor the stepped-up preparations stemmed the Russian attacks. The July 2016 attack on the DNC was followed in October by attacks on U.S. voting infrastructure. In January, the same

Kremlin-backed group also began targeting the French elections.

German officials believe that Russia will also target their upcoming elections through similar influence operations. All of this begs the question: what good is a military alliance of collective defense if it doesn't collectively defend?

This June, Stoltenberg reiterated that a cyber attack on a NATO-aligned nation could trigger an Article 5 response. But it came off as less like a warning than a marketing gimmick. "We have … decided that a cyber attack can trigger Article 5 and we have also decided and we are in the process of establishing cyber as a military domain, meaning that we will have land, air, sea and cyber as military domains. All of this highlights the advantage of being an alliance of 29 allies because we can work together, strengthen each other and and learn from each other," he said.

In general, NATO leaders appear less eager than Breedlove to go on the cyber offensive. When *Defense One* asked about the former general's comments, NATO Acting Spokesperson Piers Cazalet said, "NATO is a defensive alliance and cyber defense is part of our core task of collective defense. NATO will always act in line with its defensive mandate and in accordance with international law … 'Hacking back' is not the only possible answer to a cyber attack. The best response is to prevent the attack from happening in the first place. This is why bolstering NATO and allies' cyber defenses and resilience is a top priority."

The problem is that NATO is a military alliance, and Russian cyber and information operations are precisely designed not to provoke a military response. Indeed, that is one of the primary values of cyber operations to Russia.

This year's edition of the Pentagon's Russia Military Power report described cyber and influence operations as core capabilities, and included a section on indirect warfare. It was the first DIA Russia report since the fall of the Soviet Union. Much had changed.

"Indirect action is a component of Russia's strategic deterrence policy developed by Moscow in recent years. Its primary aim is to achieve Russia's national objectives through a combination of military and non-military means while avoiding escalation into a full blown, direct, state-to-state conflict," the report says.

This idea, commonly referred to as the Gerasimov Doctrine, is typically credited to Gen. Valery Vasilyevich Gerasimov, who leads the Russian General Staff of the Armed Forces. The doctrine lays out a framework to determine how to attack an enemy without provoking a direct military retaliation. It's war by persistent annoyance.

"Russian security and military theorists have posited in recent years that conflict has begun to increasingly be characterized by integrated military and non-military actions. Chief of the General Staff Gerasimov's article in early 2013 was one of the most prominent discussions of how these types of actions characterize modern warfare, and he explicitly claimed that the West uses such techniques. Though these articles typically ascribe 'indirect actions' to what Russia claims is the Western way of war, Moscow itself used some of these de-stabilization techniques in its operations in Ukraine," a spokesperson for the Defense Intelligence Agency said. "While the article was seized upon by some commentators as representing a new 'Gerasimov doctrine', the article is only one of numerous Russian articles discussing the increasing importance of non-military tools in modern conflict."

For Breedlove, Gerasimov's Doctrine is not just a theoretical construct, it's the reason his email was hacked. "It's active in almost every nation. This is certainly active in my nation."

Countering indirect cyber operations won't be easy. But Breedlove believes that NATO's current response stops short of even trying. That lack of resolve shows the Kremlin that the strategy is effective. "The enemy is bringing information warfare to us in all of our capitals and to us as an alliance. We have elected again to act reactively and defensively," he said. "A disruptive answer to these cyberattacks might first be a policy that will allow us to return fire to offensively take the fight to the enemy, which is what we in the military want to do. As a fighter pilot … we always say that the best defense is a good offense. If you have a missile in the air headed at your opponent, he's not worried about attacking you right now. He's worried about survival. "

- Patrick Tucker is technology editor for Defense One. He's also the author of The Naked Future: What Happens in a World That Anticipates Your Every Move? (Current, 2014). Previously, Tucker was deputy editor for The Futurist for nine years. Tucker has written about emerging technology in Slate, ... Full bio ▸

- F≡cebook
- Twi??e!
- LinkedIn
- ▸ m≡il ?his ≡!?icle

✉ Enter your email to get c Subscribe

Most Read

1. 1
   Spooked by North Korea, Lawmakers Resurrect an Old Missile-Defense Idea
2. 2
   North Korea Just Called Trump's Bluff. Here's What the US Can Do
3. 3
   As Trump and Putin Met, US and UK Defense Chiefs Discussed Ways to Deter Russia

Subscribe

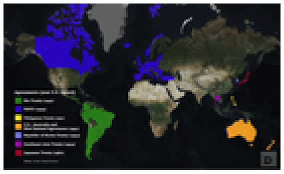
Receive daily email updates:

Subscribe to the Defense One daily.

Be the first to receive updates.

✉ Enter your email Subscribe

Don't Miss

-
  How to Deal With North Korea
-
  The Race to Build — or Stop — North Korea's Nuclear Missiles
- 
  Mapped: America's Collective Defense Agreements