#GailForce: Has the U.S. experienced the long predicted Cyber Pearl Harbor? | Lima Charlie News

limacharlienews.com (https://www.limacharlienews.com/national-security/gailforce-russia-cyberwar/) · by Gail Harris

> There is no need to wage a kinetic war or even to use debilitating cyber attacks on critical infrastructure if you can sway an election to elect a candidate or a party friendly to your interests or to defeat one you don't like.
>
> – Toomas Hendrik Ilves, President of Estonia (2006-2016)

What if in August of 2015, the FBI received credible intelligence that Russian operatives were planning to blow up the DNC headquarters building, and physically harm the Democratic Presidential candidate? What if the DNC headquarters was then attacked in June of 2016, an attempt was made to harm the Democratic nominee, and there was conclusive evidence from the intelligence community that the Russians were behind it all? What would have been the reaction of the U.S. government, the military, and the public?

In the above scenario, I'm describing what military strategists refer to as a "kinetic attack". What actually happened in June 2016 is called a "non kinetic" attack. There are many who still argue that unless death or destruction results, a cyber incident should not be considered an attack or an act of war. What they are missing is that cyber space has given nation states, or transnational groups, or single threat actors, the capability to effectively use information as a devastating weapon. The current buzzword is "weaponized narrative". As the 2014 North

Korean hack against Sony Pictures highlighted, cyber space is also a security arena where a private corporation may have to defend itself against an attack by a nation state.

During the Cold War both sides commonly used information operations to spread propaganda and narratives that made the other side look bad or to influence outcomes. Russia was always a master of disinformation. What's changed is using cyber to steal information, then marry information/propaganda with social media, then use bots and other cyber tricks to push that misinformation to a vast audience. This makes it easier to shape public opinion than in the old days. In countries such as ours that allow free speech, these operations are harder to detect and much less defend against.

As discussed a bit later, while cyber attacks on infrastructure, generally denial-of-service (DDoS) attacks, and misinformation campaigns were used against former Soviet Union countries such as Estonia (2007) and Georgia (2008), most recently, allegations have arisen that the current French elections have been tampered with in a similar manner to the DNC hack. Reports this week (https://www.washingtonpost.com/news/worldviews/wp/2017/04/25/cyberattack-on-french-presidential-front-runner-bears-russian-fingerprints-research-group-says) are emerging that a potential Russian affiliated hacker group known as "Fancy Bear," the same group accused of being behind the DNC leaks, created phishing domains to steal information from supporters of the leading candidate Emmanuel Macron. Information stolen would be then used to discredit Macron, in support of Marine Le Pen who has advocated anti-EU, pro-Russia views.

Such disinformation campaigns have become so problematic, in February UK Defense Secretary Sir Michael Fallon declared (https://www.theguardian.com/technology/2017/feb/02/nato-must-do-more-to-counter-russias-cyber-weaponry-says-fallon) that Russia was "weaponizing misinformation" to destabilize democracies and weaken NATO. Fallon pointed

to suspected Russian attacks targeting countries such as France, Germany, Bulgaria, the Netherlands, Montenegro and the U.S. He blamed Russia for targeting democracies, stating, "Today we see a country that, in weaponising misinformation, has created what we might now see as the post-truth age. Part of that is the use of cyber-weaponry to disrupt critical infrastructure and disable democratic machinery."

FBI Dir. James Comey and NSA Dir. Mike Rogers testify before House Intel Committee MAR 20, 2017

I've noticed that U.S. senior intelligence officials are quick to say they stand by their analysis (https://www.limacharlienews.com/politics-society/fbi-nsa-russia-trump-investigation/) that Russia was behind the DNC hack, an operation that resulted in the release of thousands of stolen emails, intentionally selected to include damaging information about the Democratic Party and Hillary Clinton. The CIA confirmed in December that Russian hackers also breached *Republican* party members and GOP organizations prior to the election, including Republican House members. The CIA also confirmed that entities connected to the Russian government bankrolled "troll farms" that spread fake

news about former Secretary Clinton. To put this in context, Buzzfeed reported that in the last three months leading up to the U.S. election, fake news stories were shared on Facebook 8.7 million times, surpassing mainstream news by 1.4 million shares.

In December, 2016, President Barack Obama vowed that the U.S. would retaliate against Russia "at a time and place of our own choosing" for its attempts to influence the elections. Last month FBI Director Comey and Cyber Command/NSA head Admiral Mike Rogers testified before Congress (https://www.limacharlienews.com/politics-society/fbi-nsa-russia-trump-investigation/) and not only confirmed these attacks, but said what was different about Russian influence operations during the DNC Hack was how "loud" the activity was, as if the Russians wanted us to know they were doing it. Both men said Russia would be back in 2020 and probably 2018.

Wikileaks, central to the DNC email leaks, published some quarter million U.S diplomatic cables in 2010, and just last month, published nearly 8,000 documents containing CIA materials. This prompted CIA Director Mike Pompeo earlier this month to issue a scathing announcement calling Wikileaks a "hostile intelligence agency (http://time.com/4739191/cia-director-mike-pompeo-wikileaks/)." This was soon followed by reports last week that the U.S. Justice Department is considering charging (http://www.cnn.com/2017/04/20/politics/julian-assange-wikileaks-us-charges/) Wikileaks founder Jullian Assange for, among other crimes, violating the Espionage Act.

While every U.S. intelligence agency has concluded that Russia was behind the DNC leaks, and that there is a connection to Wikileaks, what they refuse to say, at least publicly, is if the Russian influence operations caused more people to vote for the Republican candidate. They point out that it is not in their charter; they do analysis on foreign related issues.

> They'll be back in 2020, they may be back in 2018. And one of the lessons they may draw from this is that they were successful, because they introduced chaos and division and discord and sowed doubt about the nature of this amazing country of ours and our democratic process.
>
> – FBI Director James Comey, before the House Intelligence Committee, March 20, 2017

This brings me to the Pearl Harbor question. No, the DNC hack was not seen as a Cyber Pearl Harbor. There was no destruction of civilian or military infrastructure, no shutdown of power grids, transportation or banking systems, no physical injury or loss of life. But, in my opinion, it should have been seen as such an attack. A critical distinction is that the attacks on Pearl Harbor and the terrorist attacks on 9/11 were *game changers*. They were of such magnitude and effect that they galvanized public support enabling the government's decision to respond to both incidents militarily and made it easier to develop laws, rules and regulations that allowed the government to most effectively operate.

In the case of Pearl Harbor, in one day the strong isolationist sentiment and desire by Americans to not get involved in another European world war ended. In terms of military developments, prior to Pearl Harbor there was an ongoing debate in the Navy on the value of air power and the role of the aircraft carrier. Many believed battleships should remain the centerpiece of the Navy, while others, led by Rear Admiral William A. Moffett, believed that aircraft carriers should play a major offensive role. Seventy-six years later the aircraft carrier remains the centerpiece of naval strategy.

Terrorism was a major threat long before 9/11 and both the military and government agencies like the FBI had successfully dealt with it in the past. While on active duty, I was usually the first woman assigned to most of my jobs. Whenever someone came up to me and started the old "women didn't belong in

combat zones" argument, I'd remind them that terrorism was a form of warfare and an ever present threat, therefore *any* geographic location was potentially a war zone. What 9/11 did was make the general public aware of the threat and what could happen if not dealt with properly. This support allowed the government and military to take what steps they felt needed to support the war on terrorism.

I'm not seeing the same kind of widespread public support and awareness in the aftermath of the DNC hack. Additionally, Congress is in gridlock. On the Republican side there seems to be an underlying fear that if they probe too deeply, the legitimacy of the election will be questioned. On the Democratic side there seems to be a belief members of the current administration may have colluded with the Russians but they're afraid to scream too loudly for fear of being called sore losers.

This brings me to my major concern. Although there are many people in the government, military, and industry doing heroic things in dealing with the threats and issues caused by our reliance on the internet and vulnerability to cyber attacks, the general public remains unaware and/or unconcerned with the

issues and problems caused by our reliance on the internet. Since many private citizens have been victims of some form of cyber attack or harassment (revenge porn for example), this is a head scratcher for me.

Our vulnerability may have gotten even worse. Earlier this month, President Trump signed into law a measure repealing online privacy protections established by the Federal Communications Commission under the Obama Administration. By repealing these protections, internet service providers (e.g., Comcast, Verizon, AT&T), can pass on their customers' browsing habits, whom they exchange emails with, and other information, without the knowledge or approval of the consumer. Where is the public outrage? I'm very conservative in my web surfing habits but even I have gone to web sites I'd prefer to keep private. Okay, I go to my favorite soap opera site daily to see what happened today and what's going to happen next week!!!! Deal with it.

The little girl saw her first troop parade and asked,
'What are those?'
'Soldiers.'
'What are soldiers?'
'They are for war. They fight and each tries to kill as many of the other side as he can.'
The girl held still and studied.
'Do you know ... I know something?'
'Yes, what is it you know?'
'Sometime they'll give a war and nobody will come.'

– Carl Sansburg (1878-1967)

In my mind that last sentence has now changed to: *Sometime they'll give a war and only a few will notice*. There is a big gap in understanding of what cyber warfare is and is not between those frontline military troops conducting daily cyber operations and those of us sitting on the sidelines. Part of the problem can be attributed to cyber lexicon. There is still no universally agreed upon definitions of cyber war, cyber attacks, and so on among all of the world's

players to include the lawyers. Even the definition of what a "war" is can frequently get blurred. At one point in time human beings threw stones at one another and that was considered warfare.

As Peter Singer and Allan Friedman point out in their book (https://www.amazon.com/Cybersecurity-Cyberwar-Everyone-Needs-Know/dp/0199918112/ref=sr_1_1?ie=UTF8&qid=1490803087&sr=8-1&keywords=Cybersecurity+and+Cyberwar+What+Everyone+Needs), *Cybersecurity and Cyberwar What Everyone Needs to Know*, the U.S. hasn't formally declared war on another nation since 1942 when it was declared on Bulgaria. Yet since that time the U.S. has been involved in conflicts from Korea, the Cold War, Vietnam, Iraq, and Afghanistan.

NATO's Cooperative Cyber Defence Centre of Excellence has done a lot of work in this area and recently published Tallinn Manual 2.0 (https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf). As they say on their website it's written by 19 international law experts and is "the most comprehensive analysis of how existing international law applies to cyber operations." That's all well and good, but until it becomes the acknowledged standard ... well you get where I'm going.

Now I've been writing about this for years, but I submit that the US **IS** involved in an undeclared war in Cyber Space. An undeclared cyber war is also underway against our democratic, NATO allies. The DNC hack was just one part of an overall Russian strategy to destabilize the West.

Some may say Gail; the intelligence community is always exaggerating the threat cyber poses.

In a recent article (https://www.washingtonpost.com/opinions/the-united-states-must-defend-itself-against-the-real-national-security-menance/2017/03/09/6ce0c586-050a-11e7-b9fa-ed727b644a0b_story.html?utm_), Fareed Zakaria wrote, "The Defense

Department reports getting 10 million attacks a day." Critics might argue that the majority of those incidents are espionage related. I'm sure much of it is, but I'm also sure that a lot of the cyber activity and cyber attacks often dismissed should come under the *intelligence preparation of the battlefield* category. An example includes probing DoD circuits to discover weaknesses.

Critics also say that there are far more instances of criminal activity than national security threats going on. True, but what may initially look like a criminal act can turn out to be a nation state sponsored event. According to security researchers at the well regarded firm Symantic, North Korea was the culprit (http://www.npr.org/sections/thetwo-way/2016/05/27/479760450/north-korea-linked-to-81-million-bangladesh-bank-heist) in an $81-million-dollar bank heist in Bangladesh. This is the first known bank heist by a nation.

Cyber attack simulation (Norse)

Jason Healey says in his book (https://www.amazon.com/Fierce-Domain-Conflict-Cyberspace-1986/dp/098932740X), *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*:

"For over twenty-five years, nation states and non-state groups have been using computer networks to strike, spy upon, or confound their adversaries. While many of these dust-ups have been mere nuisances-more playground pranks than real battles, several incidents have become national security issues, which have placed militaries on alert and prompted warnings to heads of state, the US President included."

Healy's book should be required reading. I highly recommend it for anyone interested in cyber issues.

In March, Senator John McCain (R-AZ), Chairman of the Senate Armed Services Committee, stated (https://www.mccain.senate.gov/public/index.cfm/floor-statements?ID=1E58ECD8-94FC-4F49-AFBF-71DBE3A970AC):

"Threats to the United States in cyberspace continue to grow in scope and severity. But our nation remains woefully unprepared to address these threats, which will be a defining feature of 21st century warfare.

This committee has not been shy about expressing its displeasure over the lack of policy and strategy for deterring, defending against, and responding to cyberattacks. Treating every attack on a case-by-case basis, as we have done over the last eight years, has bred indecision and inaction. And the appearance of weakness has emboldened our adversaries who believe they can attack the United States in cyberspace with impunity. I have yet to find any serious person who believes we have a strategic advantage over our adversaries in cyberspace, and in fact many of our civilian and military leaders have explicitly warned the opposite."

Is the situation as dire as some have warned?

The West is Under Attack

As discussed earlier, suspected Russian hackers masterfully utilized cyber attacks against Estonia and Georgia, and in the case of Georgia, they followed with a kinetic attack weeks later. UK Defense Secretary Fallon warned that Russia is targeting democracies. France may be experiencing this as of this writing.

I opened with a quote from the Russian Chief of General Staff and the former President of Estonia, Toomas Hendrik Ilves. He testified before Congress (https://www.judiciary.senate.gov/imo/media/doc/03-15-17%20Ilves%20Testimony.pdf) stating,

"Virtually every history of what is now known as 'Cyber-war' or 'Cyber-warfare' begins describing an attack on Estonia at six months into my presidency in 2007 when my country's governmental, banking and news media servers were hit with 'distributed denial-of-service' or 'DDOS attacks.' Cyber attacks have a far longer history of course, but this was different. It was digital warfare, in the well-known definition of the great theoretician Carl Paul von Clausewitz as 'the continuation of policy by other means.'"

He further elaborated on Russian influence operations against NATO countries.

"All of this seems to have one goal: to weaken the NATO alliance, to weaken the European Union and European cohesion. Against a united NATO or EU, Russia is dwarfed. Against a divided Europe of individual states, or a defunct NATO, Russia dwarfs in population and in military might, even the largest of countries across the Atlantic."

Ilves pointed out that the Russians are conducting asymmetric warfare, breaking the components out:

"What are the mechanisms of this asymmetric cyber war against democracies? Kompramat, is the Russian term for publishing (real or fake) compromising materials on opponents; hacking is breaking into servers and stealing data; doxing, combines the two: to publish hacked documents to embarrass or harm opponents."

Vladimir Putin with French presidential candidate Marine Le Pen (Moscow, March 24, 2017)(Sputnik/Mikhail Klimentyev via REUTERS)

In 2008, Russian hackers used similar means (http://www.nytimes.com/2008/08/13/technology/13cyber.html) against Georgia, in what became the Russo-Georgian War. Russian hackers launched a series of DDoS attacks utilizing "zombie" computers, targeting Georgian government websites, including the president's website, before Russian ground forces invaded. Websites such as www.stopgeorgia.ru were created with a list of websites to attack, with instructions. Georgian TV, news and radio stations were hacked, and fake news websites were launched, or existing news sites were hijacked. Critical sections of Georgia's internet traffic were rerouted through servers allegedly controlled by the Russian hackers.

Just this week, reports have surfaced (https://www.washingtonpost.com/news/worldviews/wp/2017/04/25/cyberattack-on-french-presidential-front-runner-bears-russian-fingerprints-research-

group-says) that cyberattacks on the campaign offices of Emmanuel Macron, France's presidential front-runner, carried digital "fingerprints" similar to the suspected Russian DNC hack.

If Western democracies and NATO are indeed under cyber attack, are we prepared for what may come?

In February at a conference (http://westconference.org/West17/Public/Content.aspx?ID=66833&sortMenu=102001) co-sponsored by AFCEA International and the U.S. Naval Institute, VADM Michael M. Gilday, USN**,** Commander, U.S. Fleet Cyber Command and Commander, TENTH Fleet made what I thought were some very insightful observations (https://youtu.be/28godTy1Xdc) on cyber challenges in response to the question: Are We Ready to Fight – Today and in the Future.

He began by saying "it depends". He went on to point out that threats in cyber have no homeport and operate in a domain that's global. The bad guys hide in places like coffee shops in Portugal and libraries in Uganda. The attack vectors are difficult to pick up. They tend to obscure within the traffic of cyber space where there are 4 billion users online at any given time. It's difficult to sort the mix. Some of the trends that he's seeing:

- Rapid increase in number of cyber actors. This has been going on for some time.
- Rapid increase in capabilities, both the stealth and the lethality.
- Cyber tools are cheaply available to include sometimes for free.
- He's seeing a higher degree of automation particularly from proxies that operate on behalf of nation states.
- The ability to not just prey on .mil but also on .com.
- There is reverse engineering. Encryption and ransomware have flipped the cyber problem in ways we didn't think possible to hold our systems at risk.

What he believes underlies all of this is that there are no agreed upon peacetime norms in cyberspace that keep a tamp on an arms race in terms of rising numbers of actors and capabilities.

Speaking at the conference, Admiral Mike Rogers (https://youtu.be/d8WITQuOQFI), the head of both Cyber Command and the NSA said there is a need to look at cyber more broadly. He doesn't think the current break down in responsibilities between government, the private sector and the military works well. Cyber Command and the NSA are responsible for protecting military networks. They can be called upon if needed to assist in the private sector as they were when North Korea hacked Sony, but that was after the fact. You can't protect a network if you don't have the authority to monitor it.

But what about disinformation and "fake news"?

WikiLeaks founder Julian Assange (Oli Scarff/Getty Images)

Fake news is an old propaganda trick but used far more effectively in the era of social media. KGB fake news in the 1980s of AIDS being invented by the CIA had relatively little traction, but today social media disseminates false stories with abandon.

All of these have been combined in the past year as a pincer movement on democratic elections. Hacked private mail is doxed; it appears in social and later mainstream media, after which fake news content spin on these same revelations takes off and goes "viral". The Pew Center reported last Summer, that for 62 percent of Americans social media was their primary news source.

Critical to dealing with "fake news," disinformation campaigns, and cyber threats is to accept the reality that our democracy is under attack (https://www.limacharlienews.com/op-ed/trump-russia-connection/). However, there appears to be no unified "will" to solve this problem. One consequence of this lack of public involvement is that laws, rules, regulations, policies, and procedures needed to deal with cyber threats remain far behind what's needed. Cyber technology is changing at the speed of thought and laws and regulations are moving at the speed of a glacier. A coherent understanding of the threat does not exist at this time and until all sectors of our society are galvanized into action, I don't see much improvement happening quickly enough on either the national security threat cyber poses or on other cyber related issues that affect the average person.

Think I'll end here. I have no doubt that military and intelligence agencies will continue to work the problem as hard as they can but it is my hope that at some point there will be a Cyber Pearl Harbor/Wake Up Call that will galvanize the public, who will then energize lawmakers and all concerned to get on the same sheet of music and solve this very complex problem. As always my views are my own.

Gail Harris (https://www.limacharlienews.com/capt-gail-harris/), Lima Charlie News

Captain Gail Harris (U.S. Navy, Ret.), was the highest-ranking African American female officer in the US Navy at the time of her retirement in 2001. Her 28 year career in intelligence included hands-on leadership during every major conflict from the Cold War, to El Salvador, to Desert Storm, to Kosovo, and she was at the forefront of one of the Department of Defense's newest challenges, Cyber Warfare. Gail also writes for the Foreign Policy Association, is author of "A Woman's War", serves as Senior Fellow for the George Washington Center For Cyber & Homeland Security and is a Senior Advisor for the Truman National Security Project.

Follow Capt. Harris on Twitter @GailHarrisLC
(https://twitter.com/GailHarrisLC)

Lima Charlie provides global news, insight & analysis by military veterans and service members Worldwide.

For up-to-date news, please follow us on twitter at @LimaCharlieNews
(https://twitter.com/LimaCharlieNews)

limacharlienews.com (https://www.limacharlienews.com/national-security/gailforce-russia-cyberwar/) · by Gail Harris