# Security News Digest
# January 02, 2018

**It is a New Year and there is a New Quiz made for the occasion!**
**'Security New Year' Quiz**

Never mind losing weight or quitting smoking or getting more exercise – make New Year's Resolutions to learn how to protect your personal and financial information, to use security and privacy best practices, and to inform and educate other people in your life (especially those who are more vulnerable to scam artists.) And, as the last Doctor Who (The Doctor) said: Be Kind, just Be Kind.

## Canadian Government to Search Social Media Using AI to Anticipate Surges in Suicide

http://www.cbc.ca/news/canada/nova-scotia/canadian-government-to-search-social-media-using-ai-to-anticipate-surges-in-suicide-1.4467167

The Canadian government will soon hire an Ottawa-based company specializing in social media monitoring and artificial intelligence to forecast potential spikes in suicide risk. A contract with Advanced Symbolics Inc., an AI and market research firm, is set to be finalized next month. Working with the company to develop its strategy, the federal government will define "suicide-related behaviour" on social media and "use that classifier to conduct market research on the general population of Canada," according to a document published to Public Works website. This pilot project will last three months, after which the government "will determine if future work would be useful for ongoing suicide surveillance," the tender document said.

**Suicide is the second-leading cause of death for Canadians aged 10 to 19, according to the Public Health Agency of Canada.** "To help prevent suicide, develop effective prevention programs and recognize ways to intervene earlier, we must first understand the various patterns and characteristics of suicide-related behaviours," a PHAC spokesperson said in an email statement. "PHAC is exploring ways to pilot a new approach to assist in identifying patterns, based on online data, associated with users who discuss suicide-related behaviours."

**Predicting Trump, Trudeau and Brexit.** Instead of calling people to assess public opinion, **Advanced Symbolics conducts its market research by identifying and tracking social media accounts to build a representative sample of a population**. Many phone surveys poll roughly 1,500 people, but Advanced Symbolics said its representative sample of Canada's population uses more than 160,000 social media accounts. And the company said its market research method has been accurate where many others have failed. "We're the only research firm in the world that was able to accurately predict Brexit, the Hillary and Trump election, and the Canadian election of 2015," said CEO Erin Kelly.

**'We're not violating anybody's privacy'. Advanced Symbolics said its artificial intelligence looks for trends, not individual cases.** "It'd be a bit freaky if we built something that monitors what everyone is saying and then the government contacts you and said, 'Hi, our computer AI has said we think you're likely to kill yourself'," said Kenton White, chief scientist with Advanced Symbolics. Instead, the AI will flag communities or regions where multiple suicides could be likely. For example, Cape Breton Island was left reeling last year after three teenagers in the region died by suicide. "The spike that happened in Cape Breton, as unfortunate as it is, we can learn patterns from that," White said. "We can also learn patterns from what happened in Saskatchewan, patterns from Northern communities, patterns from college students." "We're not violating anybody's privacy - it's all public posts," added Kelly. "We create representative samples of populations on social media, and we observe their behaviour without disturbing it."

**Sending support before the suicides.** In the weeks following the suicides in Cape Breton, the provincial government sent additional counsellors and mental health experts to the region. **According to Advanced Symbolics, artificial intelligence could offer a two- to three-month warning before a potential spike in suicides occurs. And sharing that information with government officials could prompt them to mobilize mental health resources before a crisis, instead of afterward.** The

company will begin defining suicide-related behaviour in January, with monitoring slated to start later in 2018.

## Nova Scotia Man Who Lost Thousands in Gift-Card Scam Worries He'll Be Evicted

http://www.cbc.ca/news/canada/nova-scotia/gift-card-scam-1.4467270

A Lower Sackville, N.S., man is out thousands of dollars and worried he could be evicted after falling victim to a gift-card scam this holiday season. "They took me for a ride and I learnt the lesson the hard way," said Peter Jones, who estimates **he lost about $3,000 after buying gift cards that were later wiped clean**. Jones does odd jobs through his church, and has a service dog that helps with his depression and anxiety. He said because he was late paying his rent he received an eviction notice last week and worries his cellphone will soon be shut off. Thanks to a friend, he was able to pay December rent but still doesn't know what he's going to do for January. His landlord declined comment.

**It all started when Jones filled out an online loan form he came across on Facebook. The agency promised a loan if he provided his banking information and bought gift cards to build up his credit.** Jones's neighbour Wendy Woodrow, who realized too late what had happened and called police, said **he's not internet-savvy and trusted the Better Business Bureau logo on the document was real**. Jones said it appeared funds were being deposited into his account, so for several days he visited the nearby Shoppers Drug Mart and **bought Steam gift cards worth hundreds each. When he got home, Jones gave the gift card codes to someone on the phone. His bank eventually froze his account, he said**. "Even now Peter doesn't 100 per cent understand what's going on," said Woodrow, adding that Jones is scared that he's in trouble. "This is not his fault.... Somebody took advantage of him." The Nova Scotia RCMP said it's investigating, but admits finding culprits in cases like this is nearly impossible.

**"No reputable agency will ask a person to buy gift cards as a payment for something," said Cpl. Jennifer Clarke in an email. "If someone calls you and is asking to get access to your computer, or asks for your account numbers or passwords, it's a scam."**

Woodrow said she partially blames the Shoppers Drug Mart that sold Jones the cards several days in a row. "If there's an older gentleman who walks into the store, doesn't even know what a Steam card is, and is buying $900 at a time, like how can you guys sell this?" she asked. In an email, Loblaw Atlantic said in recent months stores have made efforts to let customers and cashiers know about potential scams, but that **scammers target the most vulnerable**. "This time of year it is not unusual for people to be purchasing gift cards as gifts so it is not possible for us to identify the purpose of every purchase," said spokesperson Mark Boudreau.

Stephen O'Keefe, a loss prevention consultant with the Retail Council of Canada, said retailers are becoming more aware of gift-card scams and often display warning signs in their stores. He said 2017 was a rough year given the large number of scams reported. "The criminals keep adapting to their environment, and so therefore we ought to as well, and that's what we try our best to do," O'Keefe said.

Jones spent Christmas with Woodrow and her family, and has been volunteering at Knox United Church where he's a member of the choir. He lost his wife last year and said he's keeping his lap dog, Zoro, close by these days. "If I go in my bedroom he follows me in, and stays right with daddy, won't leave daddy's side. He keeps me calm." *[these scams will continue because there are so many vulnerable people that need protection…]*

## Alberta Family Surprised Website Posted Obituary Without Their Knowledge

http://www.cbc.ca/news/canada/calgary/alberta-funeral-afterlife-site-1.4462877

A family in southern Alberta is raising concerns after finding a website advertising funeral gifts they didn't ask for, using an obituary containing inaccuracies about a loved one. Naomi Kimoto died on Dec. 18 in Taber, Alta. Mere hours later, her family came across her obituary posted on the "Obituaries in Taber - Alberta" Facebook page. The page links to a website called Afterlife, a company the family had never heard of nor asked to publish any information about Kimoto's death. **Afterlife's obituary page for Kimoto presents options to leave condolences, send gifts or flowers to the family for a service fee of $23.97, or light a digital, animated candle for the deceased at a cost of $4.99 to $29.99 plus GST**.

The website says this in its About Us section: "We believe that the traditional obituary should be redesigned to better reflect love at its true value and immortalize the passing of those who have left us. The collection page has been designed to simplify the sharing of memories, pay tribute to our loved ones, and communicate support to family and friends." However, Kimoto's family certainly does not feel

supported. "We're already dealing with the grief and we feel like it's an invasion of our privacy," Michelle Zeller, Kimoto's sister, told CBC News.
"My sister didn't want people to know a lot of things. She was very private about everything. So we did post something but we just posted it ourselves. **Now we don't know what the reach is going to be, I don't like the fact that it's being shared and that they're asking for flowers."** In the obituary written by the family and posted on the Southland Funeral Chapel website, it said they wanted charitable donations made if people felt so inclined, not gifts or flowers.
Zeller's daughter, Shilo Zeller, reached out to Afterlife to ask that the Facebook post and obituary be removed. It has been taken down. **In a message to Zeller's daughter, a representative for Afterlife said, "You can edit by yourself the obituary. Anyone in the world can create an obituary on the website." The representative said the obituary could not be removed from its page as someone had purchased a candle for Kimoto.**
When the family found the unwanted obituary, they contacted the owners of the Southland Funeral Chapel in Taber, who said they have nothing to do with the third-party site. Owner Darryl Gensorek said they have also made an attempt to have Kimoto's information removed from the Afterlife website. They've done the same for other chapel clients they've found listed. Gensorek said the website and its practices have "sincerely agitated" him, especially because he knows what it's like to try to help families through a difficult time. **If anything has been purchased through the website, the family says they have not received it, nor has the funeral home**.

## Necurs Botnet Fuels Massive Year-End Ransomware Attacks

http://www.securityweek.com/necurs-botnet-fuels-massive-year-end-ransomware-attacks

**The Necurs botnet started 2017 with a four-month vacation, but ended the year sending tens of millions of spam emails daily as part of massive ransomware distribution campaigns.**
**Considered the largest spam botnet at the moment**, Necurs was the main driver behind the ascension of the Locky ransomware (which in turn is associated with the Dridex banking Trojan) in 2016. As Necurs took a long vacation in the beginning of 2017, Locky was silent as well, but both resumed activity in April. Over the course of 2017, however, the botnet was involved in the distribution of the Jaff, GlobeImposter, and Scarab ransomware families, as well as in 'pump-and-dump' schemes.
Over a 10-day period between December 19 and December 29, 2017, Necurs was once again involved in the distribution of ransomware, in addition to sending typical holiday-themed scam emails, data collected by AppRiver reveals. The messages, AppRiver says, were distributing the Locky and GlobeImposter ransomware families and revealed the attackers' preference to use malicious .vbs (Visual Basic Script) or .js (JavaScript) files located inside a .7z archive. Consisting of between 5 and 6 million infected hosts and keeping around 1 or 2 million of them active at any given time, Necurs provides operators with remote access to the infected machines and can be used for various malicious activities, including malware downloads.
Starting on Dec. 19, the botnet was observed sending tens of millions of spam emails daily to distribute ransomware. It started at nearly 46 million emails on the first day (peaking at over 4.6 million messages per hour) and continued with over 47 million messages on Dec. 20 (peaking at 5.7 million per hour). While the initial spam featured mainly .vbs files inside the .7z archive, .js files started appearing as well on the second day, and the traffic switched to .js files on Dec. 21-22, when it also started to taper off, at 36 million and 29 million messages per day, respectively. The botnet remained quiet from Dec. 23-25 and recommenced activity for only a couple of hours on Dec. 26.
"Hard to say why, however, I would hypothesize the operators may have been testing or monitoring the rate of infections and realized many workers are on vacation," AppRiver's David Pickett notes. On Dec. 28-29, however, the botnet was highly active. It peaked at 6.5 million messages early morning on Dec. 28, but wasn't active for long. On the next day, Necurs was observed sending nearly 59 million ransomware messages. **The malicious emails, the security researchers reveal, were masquerading as purchase orders and voicemails, but also claimed to contain images of interest to the intended victims.**

## Teen Girl Facing Up To 10 Years for Sending Nude Selfie

https://www.hackread.com/teen-girl-facing-up-to-10-years-for-sending-selfie/

As unnerving and concerning as it sounds, the fact is that teen sexting has become a grave issue not only for the parents but also for law enforcement authorities as they often find it difficult to deal with the

situation in case something goes wrong. **According to a recent survey from Cyberbullying Research Center around 12% of teens between 12 and 17 years age sent their sexually explicit photo to someone in their lifetime and 4% of them have done so in the past month**. The latest incident involving a teenage girl being charged with the creation of child pornography is a clear proof that sexting is a dangerous act that can lend kids and teens into great trouble.

**Minnesota selfie case.** In Minnesota, a fourteen-year-old girl is being charged for sexting, which falls under the category of sexual crimes. Reportedly, the teenage girl sent an explicit selfie of hers to a boy at her school, which prosecutors claim is a violation of Minnesota's child pornography statute. Sexting is a broad term that refers to various behaviors from exchanging/sending sexually explicit text messages to suggestive videos and pictures. It is worth noting that under the statute, distribution of sexually explicit photographs of underage subjects is banned. However, in this scenario, the girl, who is being referred to as Jane Doe, sent her own picture to a boy whom she knew very well, yet, the accused is facing charges in Minnesota juvenile courts.

**American Civil Liberties Union to the rescue.** This is simply ridiculous, claims a legal brief filed by the ACLU of Minnesota; it is absurd that a teen is being charged for taking an explicit selfie because it is akin to the state charging a victim for nudity as it is exactly what the law says. According to the legal brief from ACLU, the accused sent an explicit selfie to a classmate via phone-based messaging application Snapchat and the recipient took a screenshot of the message and shared it with other schoolmates without the consent of the girl. Faribault, Minnesota police was alerted by a classmate and this is how the whole matter came to the limelight.

**The ACLU is worried because officials are charging the accused for "felony sex offense of knowingly disseminating pornographic work involving a minor to another person," a crime for which an adult would get up to seven to ten years jail time if convicted**. Though the circumstances are different since this particular case involves a teen girl, therefore the sentence might not be as harsh but it is concerning for the ACLU that **the girl would be placed on a sex offender registry if found guilty**. This would indeed be devastating for the accused of getting a job or a house will not be easy for her in the future. Jane Doe claims that she is being victimized by the state. "I'm not a criminal for taking a selfie. Sexting is common among teens at my school, and we shouldn't face charges for doing it. I don't want anyone else to go through what I'm going through," the accused stated.

As per the Minnesota statute 617,247, the purpose of child pornography law is to "protect minors from the physical and psychological damage caused by their being used in pornographic work depicting sexual conduct which involves minors." But, in this case, whether the law is applicable or not that is the whole issue. Apparently, the state is applying the law in a wrong manner since the image in question was sent by the girl with consent to a boy she liked. The case currently is being heard in Rice County juvenile court. Since the case involves a teenager, therefore, critical details of the case haven't been made public such as the accused's name and whether the accused took a photo or a video and if the boy has also been charged or not. What we do know is that the girl went to a school in Southern Minnesota.

**First Amendment.** It is also claimed by the ACLU that sexting is protected by the First Amendment because virtual child pornography was allowed while exploitation of actual children was prohibited by law, which means charging a teen for explicit selfies is itself in violation of the First Amendment, noted ArsTechnica. Moreover, it was illogical to file a case and accuse a teenager on grounds that the girl coerced herself into the creation of pornographic content because it will create another issue of limiting the expressive rights of teens.

The ACLU wrote in its legal brief: sending an explicit selfie to a peer "to indicate romantic or sexual interest, the same compelling risk of physical and psychological injury does not exist. Thus, the statute infringes upon constitutionally-protected speech." But going by the understanding of Minnesota officials, this is a case of child pornography and the teen girl could easily be classified as a child pornographer.

**This is a developing story, stay tuned**.

## That Game on Your Phone May Be Tracking What You're Watching on TV

https://www.nytimes.com/2017/12/28/business/media/alphonso-app-tracking.html

At first glance, the gaming apps - with names like "Pool 3D," "Beer Pong: Trickshot" and "Real Bowling Strike 10 Pin" - seem innocuous. One called "Honey Quest" features Jumbo, an animated bear. Yet **these apps, once downloaded onto a smartphone, have the ability to keep tabs on the viewing habits of their users - some of whom may be children - even when the games aren't being played**. It is yet another example of how companies, using devices that many people feel they can't do without,

are documenting how audiences in a rapidly changing entertainment landscape are viewing television and commercials.
**The apps use software from Alphonso, a start-up that collects TV-viewing data for advertisers**. **Using a smartphone's microphone, Alphonso's software can detail what people watch by identifying audio signals in TV ads and shows, sometimes even matching that information with the places people visit and the movies they see. The information can then be used to target ads more precisely and to try to analyze things like which ads prompted a person to go to a car dealership.**
**More than 250 games that use Alphonso software are available in the Google Play store; some are also available in Apple's app store.** Some of the tracking is taking place through gaming apps that do not otherwise involve a smartphone's microphone, including some apps that are geared toward children. The software can also detect sounds even when a phone is in a pocket if the apps are running in the background.
Alphonso said that **its software, which does not record human speech**, is clearly explained in app descriptions and privacy policies and that the company cannot gain access to users' microphones and locations unless they agree. "The consumer is opting in knowingly and can opt out any time," Ashish Chordia, Alphonso's chief executive, said, adding that the company's disclosures comply with Federal Trade Commission guidelines. The company also provides opt-out instructions on its website.
**Alphonso declined to say how many people it is collecting data from, and Mr. Chordia said that he could not disclose the names of the roughly 1,000 games and the messaging and social apps with Alphonso software because a rival was trying to hurt its relationships with developers**. (The New York Times identified many of the apps in question by searching "Alphonso automated" and "Alphonso software" in the Google Play store.) Mr. Chordia also said that Alphonso did not approve of its software being used in apps meant for children. But it was, as of earlier this month, integrated in more than a dozen games like "Teeth Fixed" and "Zap Balloons" from KLAP Edutainment in India, which describes itself as "primarily focusing on offering educational games for kids and students."
Alphonso is one of several young companies using new technologies to enter living rooms in search of fresh information to sell to marketers. **For all the talk of digital disruption in the ad world, television still attracts almost $70 billion in annual spending in the United States**, and advertisers will gladly pay to amplify and analyze the effectiveness of that spending. **The spread of these technologies, combined with the proliferation of internet-connected TVs and tools that can identify video content through pixels and audio snippets, has resulted in some questionable practices**.
Last year, the trade commission issued a warning to a dozen developers who had installed a piece of software known as Silverpush onto apps with the goal of using device microphones to listen for audio signals that humans could not hear to log what they watched on TV. This year, Vizio agreed to pay $2.2 million to settle charges that it was collecting and selling viewing data from millions of internet-connected televisions without the knowledge or consent of the sets' owners. [very long article - go to article for more]

## Five Arrested As Cops Hunt Two Of The Biggest Ransomware Strains Ever

https://www.forbes.com/sites/thomasbrewster/2017/12/20/ransomware-arrests-for-cerber-and-ctb-locker/#1a62e9f7315a

[Dec20] Five individuals have been arrested as part of an investigation into two major ransomware families - CTB-Locker and Cerber - that spread across Europe and the U.S. in recent years. All suspects were arrested in Romania, Europol announced Wednesday, as six properties were searched as part of a major global police operation involving the FBI and the UK National Crime Agency, as well as Romanian and Dutch investigators.
**CTB-Locker was one of the first ransomware strains to use the Tor anonymizing network in order to hide its command and control operations. It was also found by McAfee to be the most widespread ransomware of 2016. Criminals would typically spread it via spam containing an invoice, which, when opened, would attempt to infect Windows PCs.** It was based on the code of **CryptoLocker, previously one of the most successful ransomware variants around, until a police operation in June 2014 led to its demise, though not before it made $27 million in ransoms**.
When the police raided the homes of those they suspected being involved in CTB-Locker in the last week, they inadvertently came across what they claimed was evidence two members of the same gang were spreading Cerber, a ransomware that was focused on extorting money out of Americans. Earlier this year, Google ranked Cerber as the most criminally profitable ransomware around, having made $6.9

million up to July 2017. The two suspects were arrested in Bucharest as they were trying to leave the country, after U.S. authorities issued an international search warrant.
Europol, which helped coordinate the international police operation, released a dramatic video of the arrests, in which armed officers stormed the suspects' residence. **The Dutch police revealed that cryptocurrency mining equipment was seized, alongside laptops and hundreds of SIM cards**. The identities of the individuals arrested were not released, however.

## Forever 21 Breach Lasted Over Seven Months

https://www.infosecurity-magazine.com/news/forever-21-breach-lasted-over/

**Encryption was not turned on at some of the point of sale (POS) devices used in Forever 21 stores, exposing customers card data to info-stealing malware last year, the firm has revealed**. In an update to November revelations of a major data breach, the fashion retailer claimed that an investigation had found signs of "unauthorized network access and installation of malware on some POS devices designed to search for payment card data."
"The malware searched only for track data read from a payment card as it was being routed through the POS device," it added. "In most instances, the malware only found track data that did not have cardholder name - only card number, expiration date, and internal verification code - but occasionally the cardholder name was found." To make matters worse, encryption was turned off in some stores for over seven months - from April 3 to November 18, 2017.
The statement continued: "Additionally, Forever 21 stores have a device that keeps a log of completed payment card transaction authorizations. When encryption was off, payment card data was being stored in this log. In a group of stores that were involved in this incident, malware was installed on the log devices that was capable of finding payment card data from the logs, so if encryption was off on a POS device prior to April 3, 2017 and that data was still present in the log file at one of these stores, the malware could have found that data."
**Customers using the retailer's website were not affected, and the firm is still trying to figure out if any stores outside the US were impacted. It operates in over 50 countries worldwide, but hackers favor the US as chip and PIN has been slow to take off there, making it easier for them to steal the data and clone cards.**

## Anonymous Hacks Italian Speed Camera Database

http://www.thenewspaper.com/news/63/6369.asp

Individuals operating under the banner of the group Anonymous remotely took control of a local police computer system in Correggio, Italy, last week. After erasing the speed camera ticket database, those responsible sent screenshots of their work to various Italian newspapers to prove that they had eliminated 40 gigabytes worth of infringement photographs. According to Gazzetta di Reggio, the group also released internal emails, documents and related information to the media. "Ho Ho Ho, Merry Christmas," read the message from Anonymous, which was sent from the municipal police department's own email account.
As additional proof, the message included login information for the newly depleted "Concilia" database along with samples of the full violation data that had been accessed. The company Verbatel provided the system that integrated data for the judiciary and police in Correggio, but its security proved unreliable. Internal email messages released by Anonymous described how a municipal employee previously had to fix a "mess" by restoring the database back to December 5 - suggesting that at least some data may be available from backups.
Gazzetta di Reggio described the documents provided to reporters as including notes from two motorists complaining that they received tickets from Correggio speed cameras, even though they had never before passed through the area. Emails between police administrators and local politicians discussed how the speed camera profits were to be distributed. While this may be the most serious security lapse involving photo enforcement, it is far from the only incident. Last year, Victoria, Australia had to shut down 280 speed cameras after a ransomware virus infected the automated ticketing machines, causing them to freeze and reboot.

## Iranian Web Crackdown Drives Surge in Privacy Technology

https://news.sky.com/story/iranian-web-crackdown-drives-surge-in-privacy-technology-11191740

The use of counter-censorship technology is increasing in Iran after the authorities blocked access to popular communications services. **Photo-sharing app Instagram and encrypted messaging app Telegram have been blocked in the country despite president Hassan Rouhani claiming he would allow "space for legal criticism" as demonstrations against the clerical regime continue. Despite the potential disruption to communications provided by these blocks, the use of anonymity network Tor has increased to its highest ever number in the country.**
Metrics collected by the Tor developers show a spike in usage in recent days driving close to 9,000 users connecting to the network directly from Iran. Tor encrypts its users' internet connections and relays them through other machines, allowing people to hide their location and identity from anyone engaging in network surveillance. Metrics are not available regarding the use of Virtual Private Networks (VPNs) to route around the state's network controls, but they are known to be popular in the country.
Dr Steven Murdoch, a researcher at UCL and a contributor to the Tor Project, explained to Sky News how the Iranian authorities were able to block access to those apps. "For the vast majority of internet services, including Instagram and Telegram, a user's device must connect to a particular IP address or domain name. "A country who controls the user's internet connection can quite easily identify which IP addresses and domain names correspond to a particular service, and block them." "It takes considerable effort to design a service that is resistant to such blocking, but it is possible," Dr Murdoch said.
"Tor is one example of a technology that allows its users to browse webpages that would otherwise be blocked. Virtual Private Networks (VPN) are another approach to bypass blocking, though it is possible that VPN services will keep track of what people do and hand this information over to government." The founder and chief executive of blocked app Telegram, Pavel Durov, said that the Iranian government was blocking access to his app because the company refused to shut down discussions regarding peaceful protests. In a statement on Telegram, Mr Durov said: "We are proud that Telegram is used by thousands of massive opposition channels all over the world. "We consider freedom of speech an undeniable human right, and would rather get blocked in a country by its authorities than limit peaceful expression of alternative opinions."
[disclosure: tweets from the 45th President of the US have been edited out here as it is not about him]
Dr Murdoch told Sky News that "the instant messaging service Signal also has the ability to bypass blocking, by disguising itself amongst Google's services. This technique has been deployed in Egypt and UAE. **"However as a result of US sanctions, Google blocks users from Iran from accessing many of its services, including the one that Signal uses to resist blocking." Google did not immediately respond to Sky News for comment regarding why this service would be covered by sanctions against Iran.**

## Vietnam's 10,000-Strong 'Cyber Army' Slammed by Rights Groups

http://www.securityweek.com/vietnams-10000-strong-cyber-army-slammed-rights-groups

**The deployment of 10,000 cyber warriors to fight online dissent in Vietnam adds a grim "new dimension" to controls on free speech in the Communist country, a rights group has said.**
Vietnam routinely jails its critics and closely monitors activists on social media, which is not banned unlike in neighbouring China. A top Vietnamese general this week said a 10,000-strong brigade dubbed "Force 47" has been tasked with fighting "wrongful views" spreading on the internet, according to state media reports. It was not immediately clear what Force 47 is responsible for, but observers anticipate the cyber soldiers will escalate smear campaigns against activists online.
Human Rights Watch deputy Asia director Phil Robertson said the cyber scouts announcement was a "shocking new dimension to Vietnam's crackdown on dissent". Others said the tactic is designed to squeeze online critics. "This is just the latest plank in a campaign to curb internet freedoms at all costs," Shawn Crispin, Committee to Protect Journalists' Southeast Asia representative, told AFP Friday. "While they can't unplug Facebook, Instagram and the likes outright, they can apply more and more pressure on those platforms and it looks like these cyber troops are their latest attempt to do that."
**Vietnam's internet is classified as "not free", according to web watchdog Freedom House, which ranks it second only to China in Asia. Around half of the country's 93 million people have access to the internet, and the country also ranks among Facebook's top 10 users by numbers.**
Vietnamese officials did not respond to a request for comment from AFP. Earlier this year the government asked Facebook and YouTube to remove "toxic content" from its sites. In August, the president called for tougher internet controls, saying that groups have used the web to launch campaigns against the government that threaten the "prestige of the party's leaders and the state".

A conservative leadership in power since last year has waged a crackdown on dissidents, with at least 15 arrested this year, according to Amnesty International. Several other have been handed heavy jail terms, joining scores of activists already behind bars. Force 47 is likely to include commentators hired to publish pro-government material and counter critics, said Madeline Earp, senior research analyst with Freedom House. "Vietnam very much follows China's example when suppressing internet freedom, particularly when it comes to blocking websites and arresting dissidents," she told AFP. **For some activists, the cyber troop announcement is no surprise. But activist Nguyen Chi Tuyen said the new force marked an escalation in state tactics of repression.** "The main purpose for Force 47 is to try and control news and public opinion on the internet... they want to protect the party, not protect the country," said Tuyen, more commonly known by his online handle Anh Chi.

## China Has Shut Down 13,000 Websites Since 2015: Xinhua

http://www.securityweek.com/china-has-shut-down-13000-websites-2015-xinhua

China has shut down or revoked the licenses of 13,000 websites since 2015 for violating the country's internet rules, state media reported Sunday. The news comes as the Communist country continues to strengthen its already tight regulation of the internet, a move which critics say has picked up pace since President Xi Jinping came to power in 2012. **Platforms have also closed nearly 10 million internet accounts for "violating service protocol", the official news agency said Sunday, likely referring to social media accounts.**

"These moves have a powerful deterrent effect," Xinhua quoted Wang Shengjun, vice chairman of the Standing Committee of the National People's Congress (NPC), as saying. **Despite being home to the world's largest number of internet users, a 2015 report by US think tank Freedom House found that the country had the most restrictive online use policies of 65 nations it studied, ranking below Iran and Syria.**

**This year alone, it has enacted new rules requiring foreign tech companies to store user data inside the country, imposed fresh content restrictions, and made it increasingly difficult to use software tools that allow users to circumvent censors. Google, Facebook, Twitter and The New York Times are all blocked in China, among countless other foreign websites.**

Beijing strictly defends what it calls "cyber sovereignty" and maintains that its various forms of web censorship - collectively known as "The Great Firewall" - are necessary for protecting its national security. Within China, websites must register with authorities and are responsible for "ensuring the legality of any information" posted on their platforms, according to regulations in force since 2000. When their content runs afoul of authorities, they can be shut down or fined. One way to bypass the strictly controlled domestic internet is by using a virtual private network (VPN) which can allow users to access the unfiltered global internet. But here too authorities have cracked down. Earlier this week, Wu Xiangyang from the southern Guangxi Zhuang autonomous region was sentenced to five and a half years in prison for selling a VPN service on Alibaba's Taobao and other marketplaces.

**********