A NEW WAVE OF CYBER VILLAINS

HUGINN WHITE PAPER

A new wave of cyber villains

By Huginn Team

In information theory, the notion of information may often be seen as a mathematical quantity, and indeed, the information industry has largely relied in its operations on this definition of the term. But information can, with good reason, be understood as being much more than this. The Oxford Dictionary of English defines information firstly as the 'the facts provided or learned about something or someone: a vital piece of information'.

Manipulation, on the other hand, is described as 'the action of manipulating something in a skilful manner' or 'manipulating someone in a clever or unscrupulous way'. The act of manipulating is 'to handle or control (a tool, mechanism, information, etc.) in a skilful manner' or 'control or influence (a person or situation) cleverly or unscrupulously'. Many of the threats present today are painted as information sabotage, which can be seen as the use of manipulation for the purpose of 'destroying, damaging, or obstructing something, especially for political or military advantage' – that is, for activities that fall under the conventional rubric of sabotage.

> *"It is the notion of 'vitality' in the definition presented above that hints at a crucial yet surprisingly neglected aspect of information: the human dimension – that in order to be information rather than data, information must mean something to someone."*

We at Huginn believe that the aims and effects of cyber security can be far subtler than prevention of sabotage. We believe that a specialized view of information is too limiting. Information in this context is, indeed, facts provided or learned about something or someone. In our view, cyber security is, in broad terms and somewhat paradoxically, not about protecting all information. It is about protecting vital information. It is the notion of 'vitality' in the definition presented above that hints at a crucial yet surprisingly neglected aspect of information: the human dimension – that in order to be information rather than data, information must mean something to someone. Thus, our aim is to preserve the integrity of information and to prevent its manipulation.

In the following pages we will explore the current situation in cyber security and information manipulation. We also show how the situation relates to our view of security.

Gigantic resources or a bit of resourcefulness?

In our view, working within the confines of ready-made terms and disregarding the wider phenomena can lead to overly simplified security solutions, to blindsided decisions. Considering the term information sabotage hinted at above, we naturally find an abundance of breaches that fit the description neatly. However, in some cases our neat definitions are not up to the task.

Perhaps the most conventional form of information sabotage takes place when the actions are instantiated by governments or at least serve their needs. In these instances, we can speak of a goal, possibly to gain political or even military advantage. For a western reader, for instance, much of the threat is seen in the actions allegedly originating from the Russian government.

"In our view, working within the confines of ready-made terms and disregarding the wider phenomena can lead to overly simplified security solutions, to blindsided decisions."

In June 2017, it was revealed that the Russian cyber hacks on United States electoral system required an unprecedented step from the Obama administration; according to Bloomberg[1], the administration had complained 'directly to Moscow over a modern-day "red phone"'. Bloomberg states that the Russian hackers hit systems in a total of 39 states. The breach involved incursions into voter databases and software systems. Russian officials have denied any role in the cyber attacks. Regardless of who is responsible for the attack or how effective the attack was, its main achievement was in the fact that it compromised the public's view of the system's reliability. In a western democracy, the event of the voting system becoming compromised is likely to have severe consequences on the election. Even casting reasonable doubt over the electoral system can affect the political outcome negatively.

It must be added that, even though we have recently been reading about the cyber attacks on the United States election, a previous major news phenomenon was about how some western governments were spying on their own citizens. In 2013, Europe and the United States were roaring over the NSA scandal that originated from documents leaked by Edward Snowden.

The leaks related to the scandal continue to pour out to the public: in April 2017 the hacker(s) with the title Shadow Brokers leaked a dump of nearly 300 megabytes worth of materials that were described

[1] Bloomberg Politics. Michael Riley and Jordan Robertson, June 13. 2017. Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections

as National Security Agency's weaponized software exploits[2]. The exploits were described as zero-day exploits, but in fact they were fixed by Microsoft roughly a month before the dump. According to Ars Technica, the exploit weapons included compiled binaries for exploits that targeted vulnerabilities in a long line of Windows operating systems, including Windows 8 and Windows 2012. The dump also contained code for hacking into banks, particularly those in the Middle East. Included was also software for an implant tool and backdoor for controlling hacked computers through an HTTP-based command server. Many antivirus softwares at the time did not detect the software allegedly stolen from the NSA. However, even if Microsoft would have been late with the fixes, many firewall programs would have prevented most of the attacks. Some of the exploits could be prevented by company best practices that call for remote desktop connections to require use of a virtual private network.

It is worth noting that, even though the tools released by Shadow Brokers can be seen as breaches in cyber security, the way Shadow Brokers most probably accessed them is, in fact, through a breach in cyber security. The creators of malware such as Petya, WannaCry and Trickbot, were at least familiar with National Security Agency (NSA) hacker tools such as EternalBlue and DoublePulsar. These tools were revealed by Shadow Brokers[3] as well. We will return to these malware later in this white paper.

"Software alone is not sufficient when solving crimes. A hoax was devised by two resourceful cousins with a little knowledge of money transfers and access to information and data."

The case of election hacking and the NSA scandal can be seen as prime examples of 'conventional' information manipulation. It is also worth noting that security threats can be prevented by being well-equipped against attacks with effective software. Moreover, some applicable and operable practices can be sufficient in preventing some security threats.

What has been discussed above are examples of information manipulation allegedly conspired by massive organizations. It is not the case in most examples of information manipulation. This is what we will turn attention to next.

The Verizon Data Breach Digest 2017[4] gives a case study of an elaborate security system breach, which involved no coding, but resulted in damages worth nearly £500 000 (more than $650 000).

[2] Ars Technica, Dan Goodin. April 14 2017. NSA-leaking Shadow Brokers just dumped its most damaging release yet https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/

[3] ZDNet, Steven J. Vaughan-Nichols. May 17, 2017. How WannaCrypt attacks. http://www.zdnet.com/article/how-wannacrypt-attacks/

[4] Verizon Data Breach Digest 2017. http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017/ See also Bleeping Computer, Catalin Cimpanu. May 10, 2017 UK Water Supplier Loses £500,000 in Sophisticated Scam https://www.bleepingcomputer.com/news/security/uk-water-supplier-loses-500-000-in-sophisticated-scam/

The case study reveals that an unnamed regional water company based in the United Kingdom was the victim of a sophisticated scam that involved social engineering, an inside man, and international bank transfers. The company's clients had notified them that their online account details had changed. When customers had their passwords reset and regained access to their accounts, many noticed that the registered bank account details had also been changed. This meant that refunds due to the customers had been transferred fraudulently to new bank accounts. It was later determined that the refunds - totalling over £500,000 - were directed to two bank accounts in England. Later it became clear that the banks had also been socially engineered. Believing the refunds to be foreign deposits, they allowed the account holder to transfer 90% of the money to accounts in Dubai and the Bahamas as soon as the payments arrived in their UK account. Ultimately, the funds had been withdrawn from the accounts and used to purchase Bitcoin, which was transferred to addresses associated with a Bitcoin mixing (money laundering) service. Despite a robust security posture, none of the water company's security appliances or log sources showed any signs of compromise.

The investigation of this hoax led to India, where the company had outsourced its call-centre. It became evident that one user had accessed all the accounts that had been fraudulently refunded. The user denied any knowledge of the fraudulent activity and suggested the computer must have been hacked. While no evidence could be found right away on the computer, shadow copies of data were recovered, which led to the revelation that numerous email messages had been exchanged between the call center employee and another individual, later identified to be his cousin in the UK. These emails contained pictures of account details that correlated to the accounts affected by the fraudulent activity.

The detective story above clearly displays the fact that software alone is not sufficient when solving crimes. The hoax was devised by two resourceful cousins with a little knowledge of money transfers and access to information and data systems. Neither does a successful cyber security breach always require specialized software; for this case is nevertheless a breach in the operative data systems of the company. While not knowing the specifics of this case or the data systems, we nevertheless believe that a hoax such as this can be prevented through company practices. Possible guards against these kinds of hoaxes include multi-factor authentication, monitoring network activity, observing the integrity of company core data as well as maintaining a company culture that prevents any kind of lapses in security.

Ransom or bank robbery?

In the cases of election hacking or global citizen surveillance we may see sabotage working in the traditional sense. What happened with the unnamed water supply company showed that information manipulation can be utilized for financial gain. Ransomware is perhaps one of the most widely known cyber security threats today, and more often than not, works in order to gain financial benefit to the attackers. Ransomware is often sabotage: it takes your computer hostage, destroys much of it and takes control of your information.

One illustrative example of this brand of activity has been with us since 2016; the ransomware family Petya has wreaked havoc particularly in Microsoft Windows-based systems. In June 2017, The Guardian[5] reported that the Petya ransomware has caused serious disruption in the operations of large corporations including the advertising giant WPP, French construction materials company Saint-Gobain and Russian steel and oil firms Evraz and Rosneft. The Finnish National Cyber Security Centre Finland (NCSC-FI) deemed that ripples of the pandemic had reached Finland[6] as well. The ransomware spread aggressively in the infected companies' internal network. The latest occurrence of Petya runs for overwriting the master boot record of the computer and restarts the computer an hour after the infection. The user's files are encrypted. Infected computers display a message demanding a Bitcoin ransom worth $300. The epidemic was first reported in Ukraine, where it is believed to have originated through an update of the accounting programme M.E.Doc. It is believed that the update servers of the programme had been compromised.

Only a month before Petya, another outbreak was after the same sum of ransom. WannaCry, or WanaCrypt0r tried to extort the owners of the infected computers $300. The ransomware spread through more than 150 countries and infected hospitals, businesses and government systems[7]. In all, it was reported that the ransomware impacted over 10 000 organizations and 200 000 individuals[8]. The outbreak was stopped swiftly through a cyber expert discovering a "kill switch". Nevertheless, some users did succumb to paying the ransom. The Bitcoin accounts that held the ransomware's profits were drained. It is not known who emptied the accounts and why.

Getting money through blackmail is often a risky effort. In WannaCry's case, hundreds of thousands of compromised computers yielded payments of roughly 140 000 dollars. This would mean that, out of the hundreds of thousands victims, only less than five hundred paid the ransom. The amount of money is significant, but the effort may almost seem wasted in comparison to the enormity of the campaign. Two resourceful cousins were able to steal a lot more. Bank robbery could occur to be much more profitable. This is the goal that cyber attack campaigns against banks aim for.

[5] The Guardian, Jon Henley and Olivia Solon. June 27 2017. 'Petya' ransomware attack strikes companies across Europe and US. https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe

[6] FICORA. 27 June 2017. Petya-kiristyshaittaohjelma leviämässä nopeasti. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/06/ttn201706271729.html

[7] CNN Tech, Selena Larson. August 3, 2017. Someone has emptied the ransom accounts from the WannaCry attack. http://money.cnn.com/2017/08/03/technology/wannacry-bitcoin-ransom-moved/index.html

[8] The Verge, Andrew Liptak. May 14, 2017. The WannaCry ransomware attack has spread to 150 countries. https://www.theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware-attack-spread-150-countries

> “... we can, and should, imagine what would happen if these crude campaigns would become much smarter. We can only speculate how large the financial effect would be if the malware would be able to manipulate the information in enterprise resource planning systems such as SAP.”

During the summer 2017, the banking trojan Trickbot had learned new tricks. It had developed the ability to steal the identities of different banks, and through that, steal the credentials of the banks’ customers[9]. Through a phishing email, the attackers were able to infect their victims’ computers. Once a computer was infected with Trickbot, the malware ran in the background and waited for the victim to visit their online bank. When they did so, Trickbot redirected them to a malicious site, which in this case is a fake version of the banking website that looks exactly like the real thing – complete with the correct URL of the online bank and a legitimate SSL certificate, so a user may not suspect they’re being tricked. The URL field of the web browser is often the last safety net for a web user. For example, some Apple ID phishing operations are prevented because the users are alarmed by the URL of the site the phishing emails lead to[10]. According to ZDNet, it’s currently not clear who is behind Trickbot, but the way the malware is continually evolving suggests it’s the work of a well-organized, well-funded cybercriminal group.

As was stated above, massive malware campaigns do not necessarily yield wide financial benefits for the actors behind the campaigns. In a word, the campaigns are badly designed. Yet we can, and should, imagine what would happen if these crude campaigns would become much smarter. After all, even Trickbot has been able to learn. Were the malware to somehow learn information manipulation skills, the outcome would be much more severe. We can only speculate how large the financial effect would be if the malware would be able to manipulate the information in enterprise resource planning systems such as SAP. In fact, sometimes getting access to the enterprise systems would not even require any software, as other avenues of identity theft could be exploited.

Darkness or trust?

In warfare, sabotage may involve attacks on the supply systems of the enemy states. The industrial sector is a prime target. In September 2017, Symantec warned that the energy sector in Europe and North America is being targeted by a new wave of cyber attacks that could provide attackers with the

[9] ZDNet, Danny Palmer. August 14, 2017. New Trojan malware campaign sends users to fake banking site that looks just like the real thing. http://www.zdnet.com/article/new-trojan-sends-users-to-fake-banking-site-that-looks-just-like-the-real-thing/

[10] FICORA. January 5, 2017. Apple ID -huijaussivustot pyrkivät varastamaan pankki- ja luottokorttitiedot - suomalaisuhreja kymmeniä päivittäin. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/01/ttn201701050945.html

means to severely disrupt affected operations[11].

Symantec claims that the group behind these attacks is known as Dragonfly. The group has been in operation since at least 2011 but has re-emerged over the past two years from a quiet period following exposure in 2014. This “Dragonfly 2.0” campaign, which appears to have begun in late 2015, shares tactics and tools used in earlier campaigns by the group. Again, a phishing campaign as well as trojanized software and watering hole websites were utilized. According to the Guardian[12], Dragonfly’s methods are varied, but all its attacks seem to be focused on researching the inner workings of energy firms. It has been seen sending malicious emails with attachments that leak internal network credentials, which are then used to install backdoors on the network allowing the hackers to take control of computers and systems. They’ve also been seen seeding fake flash updates to install the backdoors and carrying out “watering hole” attacks, hacking third-party websites that were likely to be visited by people working in the energy sector. Symantec reminds us that the energy sector has become an area of increased interest to cyber attackers over the past two years. Most notably, disruptions to Ukraine’s power system in 2015 and 2016 were attributed to a cyber attack and led to power outages affecting hundreds of thousands of people.

“Security culture is not something that can be outsourced to a single department in the company. In our view, security management should be regarded as an integral aspect of business management.”

Banks are also very attractive targets to cyber-crime. In November 2016, it was reported[13] that Tesco bank had spotted suspicious transactions on around 40 000 accounts, and that money was taken from around 20 000 customers. Many account holders reported losing hundreds of pounds. Tesco Bank did not say how much money is involved in total, although Bloomberg[14] states that the bank had to spend more than 2.5 million pounds ($3.3 million) reimbursing almost 10 000 customers whose accounts were hacked. The bank says it fell victim to online criminal activity. Cliff Moyce, global head of financial services at technology firm DataArt told the Guardian, that the chance of the problem being cause by a “remote technical hack” was less than 50%. “Far more likely is the (in)action of a human actor, or weak process/management controls when information is shared between providers,” he said. Moyce said Tesco would need to investigate the possibility of an “economic hack” in which an offshore

[11] Symantec Security Response. September 6, 2017. Dragonfly: Western energy sector targeted by sophisticated attack group. https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group

[12] The Guardian, Alex Hern. September 6, 2017. Hackers attacking US and European energy firms could sabotage power grids https://www.theguardian.com/technology/2017/sep/06/hackers-attacking-power-grids-in-us-and-europe-have-potential-to-sabotage

[13] The Guardian, Hilary Osborne. November 7, 2016. Tesco Bank fraud: key questions answered. https://www.theguardian.com/money/2016/nov/07/tesco-bank-fraud-key-questions-answered-suspicious-transactions-40000-accounts

[14] Bloomberg Gadfly, Edward Evans. July 26, 2017. Bankers vs. the Black Hats. https://www.bloomberg.com/gadfly/articles/2017-07-26/unicredit

employee is offered a large sum of money in return for a tranche of customer data.

Two years previously, the Bank of England warned that banks were not taking the threat of cyber-attacks seriously enough, and experts have warned that they could fall victim to different types of fraud. But so far there have been no other attacks on the scale of that reported by Tesco. In January 2016, HSBC customers were locked out of online banking after the company was targeted in a "denial of service" attack. This brought down the website, but there were no reports of any losses to customers following the attack.

The danger in cyber-attacks against banks extends to much more than money. If the attacks manage to damage the public's view of the banks and if the public sees the banks as unreliable, the business effects may be irrevocable. Tesco's stock took a hit of as much as 3.3 percent[15] after it was forced to suspend online actions. In a sense, Tesco bank was a newcomer; Tesco has only offered checking accounts since 2014 and then mostly through its website or mobile app. While established banks are not safe from information manipulation, in some aspects they have a longer heritage of a company culture where they are aware of the possible threats posed to banking. We have to stress the importance of company culture. Good security culture may prevent information manipulation against banks. However, security culture is not something that can be outsourced to a single department in the company. In our view, security management should be regarded as an integral aspect of business management.

> *"The attackers behind Carbanak picked banks that were weak and poorly secured and took their time. The result was at least $300 million and possibly $1 billion stolen from the banks."*

Much of the breaches we have described above have not been very 'smart', and the financial benefits of the attackers have been relatively small. They may of course have affected the businesses seriously. However, if we extend our perspective to a few more years in the past, we can see how large the amounts of money stolen can be. These attacks were in the works for extended periods of time. Here we can also see the scale of what the effects can be when subtle and gradual information manipulation is utilized. The attackers behind Carbanak[16] picked[17] 30 Russian, Ukrainian, Chinese, US and German banks that were weak and poorly secured and took their time. They started by infecting the bank, ending up with hundreds of infected machines. They harvested intelligence and started mimicking staff behavior. They started stealing money through online banking, e-payment systems, inflating account balances and

[15] Bloomberg Gadfly, Lionel Laurent. November 7, 2016. https://www.bloomberg.com/gadfly/articles/2016-11-07/tesco-bank-hack-will-be-warning-to-fintech-s-upstarts

[16] Kaspersky Lab. February 16, 2015. The Great Bank Robbery: the Carbanak APT. https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/

[17] Computerworld UK, John E. Dunn. February 16, 2015. The $1 billion 'Carbanak' bank heist - how it was done. https://www.computerworlduk.com/it-vendors/huawei-looks-to-give-indoor-mobile-speeds-a-boost-with-lte-advanced-3598097/

controlling ATM's. The result was at least $300 million and possibly $1 billion stolen from the banks.

While not particularly subtle, information manipulation was involved in a reportedly[18] state-sponsored bank heist that resulted in $81 million being stolen from the Bangladesh central bank's account at the New York Federal Reserve in February 2016. The attackers were able to breach Bangladesh Bank's systems and used the SWIFT messaging network to order the transfer of nearly $1 billion from its account at the New York Fed. The U.S. central bank rejected most of the requests but filled some of them, resulting in $81 million being transferred to bank accounts in the Philippines. The money was quickly withdrawn and later disappeared in the huge casino industry in the country. In March 2017 Reuters[19] reported that the FBI believed North Korea was behind the heist.

The home fires can stop burning

In the case of Tesco bank we saw a relatively fresh business model being attacked. While innovation, new services and new technology can improve our lives, they also bring up new threats. The home is regarded by most as a safe haven, where nobody should be able to enter without permission nor use the home without consent.

We at Huginn are from a country where the climate can be very harsh during the winter season; a warm home is essential for survival. We would not want the heating of our homes suddenly shut down. Yet this has already happened through cyber-attacks. During the early winter 2016, two real estate properties in Lappeenranta, Finland went cold because of a DDoS attack against the computer that controlled the heating of the properties[20]. It was reported that the computer had been connected straight to a public network without proper security measures[21].

Even if you are able to enjoy the warmth of your home from your sofa watching TV, or spending time on your mobile device or computer, perhaps editing photos while your laundry machine and dishwasher

[18] Reuters. March 29, 2017. Bangladesh Bank heist was 'state-sponsored': U.S. official. https://www.reuters.com/article/us-cyber-heist-philippines/bangladesh-bank-heist-was-state-sponsored-u-s-official-idUSKBN1700TI

[19] Reuters. March 22, 2017. U.S. may accuse North Korea in Bangladesh cyber heist: WSJ. https://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea/u-s-may-accuse-north-korea-in-bangladesh-cyber-heist-wsj-idUSKBN16T2Z3

[20] TiVi, Suvi Korhonen. November 7, 2016. Verkkoisku kylmensi useita taloja Suomessa – ES: "Lämmitys ja kuuma vesi pois päältä" http://www.tivi.fi/Kaikki_uutiset/verkkoisku-kylmensi-useita-taloja-suomessa-es-lammitys-ja-kuuma-vesi-pois-paalta-6597180

[21] Mikrobitti, Jori Virtanen. November 7, 2016. Hakkerit iskivät Lappeenrannassa kiinteistöjen lämmönjakeluun – Tuhat muuta kohdetta tiedossa? https://www.mikrobitti.fi/2016/11/hakkerit-iskivat-lappeenrannassa-kiinteistojen-lammonjakeluun-tuhat-muuta-kohdetta-tiedossa/

take care of their chores, you may be involved in a cyber attack. There are numerous reports[22], where home appliances such as air source heat pumps, televisions, cameras and home appliances are hacked and participate in distributed denial of service attacks. In February 2016, Risk Based Security[23] reported that there are more than 36 000 to 46 000 affected digital video recording units that were exposed via the manufacturer leaving hardcoded root credentials on the devices.

As we see this, the Internet of Things may make our lives easier and more comfortable. The downside is that it provides a massive amount of new targets for information manipulation. The threat is brought to our homes.

"We have a good chance of safeguarding what is most valuable to us."

Business activities in the internet can lead to tangled discussions on ethics. For example, some have criticized River City Media as a leading spam operation. Disregarding the ethics issues, we may look at a leak where River City Media files were exposed as an interesting phenomenon, where the aspiration to "be safe" caused a breach in security. It also sparked law enforcement interest into their operations. On March 2017 it was revealed that the company's entire operation was exposed because River City Media failed to safeguard backups of its database of 1.34 billion email accounts, resulting in all that user information being available for anyone to see[24]. The reason for exposure was reported to be a faulty Rsync setup[25].

MacKeeper[26] described River City Media as a "massive, illegal spam operation". The end result of the leak was, a "tangible threat to online privacy and security as it involves a database of 1.4 billion email accounts combined with real names, user IP addresses, and often physical address." MacKeeper goes on to add, that "Chances are that you, or at least someone you know, is affected." Again, the exposé was caused by a breach in cyber security. The whole issue with River City Media may raise interesting discussion over the ethics of breaches in cyber security: sometimes the results of such a breach may be regarded as positive by the wide public, other times not.

[22] Check Point Software Technologies. January 7, 2016. New Check Point Report Reveals How Hackers Can Outsmart Smart TVs. https://www.checkpoint.com/press/2016/new-check-point-report-reveals-hackers-can-outsmart-smart-tvs/

[23] Risk Based Security. February 18, 2016. https://www.riskbasedsecurity.com/2016/02/hardcoded-root-credentials-in-multiple-dvrs/

[24] Fortune, Jonathan Vanian. March 6, 2017. Major Spammer Accidentally Leaks Data on a Billion People. http://fortune.com/2017/03/06/spammer-leaks-data/

[25] CSO, Steve Ragan. March 6, 2017. Spammers expose their entire operation through bad backups. https://www.csoonline.com/article/3176433/security/spammers-expose-their-entire-operation-through-bad-backups.html

[26] MackKeeper. March 6, 2017. Spammergate: The Fall of an Empire. https://mackeeper.com/blog/post/339-spammergate-the-fall-of-an-empire

Is anything safe?

At this stage it is possible to state the question: is there anything that is truly safe in our internet-based world? Our short answer is: no. Our long answer is: while nothing is entirely safe, we can take measures that make our world safer. Despite the uncertainties, we have a good chance of safeguarding what is most valuable to us.

As has been shown, conventional cyber threats can paralyze operations and cause loss of money. However, what we have also wanted to bring forth is the idea that when the breaches involve some smart information manipulation, the losses possibly amount to billions. In addition, while conventional attacks may result in temporary paralysis, paralysis achieved through information manipulation can be much more persevering.

> *“What we propose is that there are ways of protecting the information and maintaining the integrity of information.This is what our Huginn concept aims for..”*

Indeed, already in 2015 US intelligence chiefs warned the Congress that the next phase of escalating online data theft is likely to involve the manipulation of digital information. The then US director of national intelligence, James Clapper[27] stated that he believed the next push on the envelope is going to be the manipulation or the deletion of data which would of course compromise its integrity.

In our view, information is not data. Information is data that is provided with context. Sometimes getting rid of the context is sufficient to destroy all operations. Sometimes it is sufficient to manipulate the information to achieve other, possibly financial benefits. What we propose is that there are ways of protecting the information and maintaining the integrity of information. This is what our Huginn concept aims for. We shall explore the concept in more detail in our white papers Defence in Depth and What is Huginn?

[27] The Guardian, Spences Ackerman. September 10, 2015. Newest cyber threat will be data manipulation, US intelligence chief says. https://www.theguardian.com/technology/2015/sep/10/cyber-threat-data-manipulation-us-intelligence-chief