
# MANUAL: COUNTERING DISINFORMATION and PROTECTING CYBERSPACE

Manual for Liberal Stakeholders

Péter Krekó Alice Stollmeyer Veronika Víchová Alexey Yankowski
Editor: Adéla Klečková
2019

**Authors:**
Péter Krekó
Alice Stollmeyer
Veronika Víchová
Alexey Yankowski

**Editor:**
Adéla Klečková

**Countering Disinformation and Protecting Cyberspace**
Manual for Liberal Stakeholders

Friedrich Naumann Foundation for Freedom
Jugoslávská 620/29, Praha 2 Vinohrady, 120 00

fnf-prag@fnst.org
www.fnf-europe.org/prague/

European Liberal Forum asbl.
Rue des Deux Englises 39, 1000 Brussels Belgium

info@liberalforum.eu
www.liberalforum.eu

ISBN 978-80-270-5561-6

Published by the European Liberal Forum asbl with the support of Friedrich Naumann Foundation. Co-funded by the European Parliament. Neither the European Parliament nor the European Liberal Forum asbl are responsible for the content of this publication, or for any use that may be made of it. The views expressed herein are those of the authors alone. These views do not necessarily reflect those of the European Parliament and/or the European Liberal Forum asbl.

# ABOUT

## European Liberal Forum

The European Liberal Forum (ELF) is the foundation of the European Liberal Democrats, the ALDE Party. A core aspect of our work consists in issuing publications on Liberalism and European public policy issues. We also provide a space for the discussion of European politics, and offer training for liberalminded citizens. Our aim is to promote active citizenship in all of this. Our foundation is made up of a number of European think tanks, political foundations and institutes. We work throughout Europe as well as in the EU Neighborhood countries. The youthful and dynamic nature of ELF allows us to be at the forefront in promoting active citizenship, getting the citizen involved with European issues and building an open, Liberal Europe.

## Friedrich Naumann Foundation for Freedom

In 2004, central European and Baltic countries joined the European Union as new members. Even though not in all countries pluralistic and free-market-oriented institutional structrues are completely established many of these countries are demonstrating remarkable reforms in their economies and societies. Our FNF office in Prague supports particularly the network 4liberty.eu serving as a center of competence and platform for dialogue. Network members are developing reform concepts and policy papers that are relevant for nationals and European decision makers. Core subjects are increasing the attractiveness and acceptance of a free and open society, consolidating public budgets, reforming the social security systems, integrating minorities and fighting nationalism and euroscepticism.

# CONTENT

# INTRODUCTION

Alice Stollmeyer
Executive Director at Defending Democracy Institute

Who wouldn't want to read a real page-turner? An action thriller smartly combining historical, spy and science fiction? Except... This is not a novel. This is actually happening – now. In our world, our societies, our lives. And those who think or hope it is just a bad dream had better wake up fast and face reality.

Putin's Russia has launched a hybrid war against the West – a war against our fundamental freedoms and values (democracy, rule of law, human rights) and our way of life. While (some, not all of) our governments are slowly grasping the scale and urgency of the threat, they have yet to form a clear, comprehensive, united, and strong enough response.

The enemy wants to disrupt our society, discredit our institutions and undermine our confidence so that we turn against ourselves. The return of illiberal, nationalist and xenophobic politics – often funded by Moscow – suggests that we may be losing the battle. The ability of pro-Kremlin hackers, disinformation campaigns and unaccountable algorithms to corrupt our social media, our search engines, and even social movements poisons the lifeblood of our democracy. The war on the West – both from the outside and from the inside – is a war on truth. Everything we hold dear is at risk: our trust in the rule of law; our trust in public institutions and fair elections; our trust in research and science; our trust in journalism and media; and perhaps most of all, our trust in a shared sense of decency and social cohesion.

As the very foundations and functioning of our societies are at stake, it is our duty – as patriots and as concerned citizens – to defend our societies, our freedoms and rights. Join the growing movement of freedom fighters and democracy defenders. Don't remain the silent majority – become the loud majority.This timely report gives you the information and tools you need to take action, both to counter disinformation and to help protect the cyber space. Whether you are a politician, a civil servant, or a concerned citizen, read this report like a Scout Handbook on how you get to play the good guy.

May the good guys win.

# HYBRID WARFARE 1.0

Veronika Víchová
Kremlin Watch Director at European Values Think Tank

## 1 Strategies of hybrid warfare

The term hybrid warfare has been used with increasing frequency in the last few years, especially since the annexation of Crimea by the Russian Federation and the start of the war in Ukraine. As a result, the number of definitions is rising, but in practice, the countries which are members of organizations like the North-Atlantic Treaty Organization (NATO) or the European Union (EU) do not have a common perception of what exactly hybrid warfare is and which instruments it includes.

According to the terminology used by NATO, hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives. NATO has a comprehensive approach to hybrid threats, it considers the orchestration of diplomacy, political interaction, humanitarian aid, social pressures, economic development, and savvy use of the media and military force to be part of hybrid warfare, as long as more than one of these tools is being employed.

Joshua Stowell, editor of Global Security Review, describes hybrid warfare similarly for the Global Security Review. He uses an alternative term of nonlinear war, which means that the adversary employs conventional and irregular military forces in conjunction with psychological, economic, political, and cyber assaults. Confusion and disorder ensue when weaponized information exacerbates the perception of insecurity in the populace as political, social, and cultural identities are pitted against one another.

The context of hybrid warfare is important to understand also because some of its aspects blur the difference between war and peace. It can be used by adversaries which are not in direct conflict, is often very difficult to attribute to a specific actor, and can be used by state and non-state actors alike. In this brief, the focus is going to be on the following set of the main non-military tools which are being considered as possible instruments of hybrid warfare used by adversaries against European countries:

Political Interaction
Economic Operations
Diplomacy

It is important to understand that none of these tools is strictly autonomous and that the hybrid warfare operations always consist of at least two of the instruments mentioned above, usually designed to complement each other.

### 1. 1 Information operation

The fact that information can be weaponized is not a new revelation or even a phenomenon of the 21st century.

However, new technologies, open media market and a growing number of people using social media platforms have made it significantly easier to use information to influence significant parts of society without leaving much of a trace.

Tactics of information warfare have changed accordingly. Nowadays, the disinformation campaigns and propaganda are focused on undermining the trust of the citizens in Western countries, the democratic institutions and traditional media and abusing already existing problems and issues dividing those societies.

There are a lot of misconceptions about disinformation in general. Partly this is the result of overusing terms like fake news, which are gradually losing any substantial meaning. Disinformation can be a single piece of news or communication which in some rare cases can have the potential to change public opinion or even mobilize significant portions of a population. One of the most famous examples of this type of disinformation is the so-called crucified boy (https://www.news24.com/World/News/Russian-TV-show-Ukraine-child-crucifixion-20140714) which took place in Ukraine.

Russian TV channel broadcasted an interview with a woman saying that she witnessed Ukrainian armed forces executing a little boy and then publicly crucifyxing in Slovyansk. https://www.stopfake.org/en/lies-crucifixion-on-channel-one/ The story has been disproven several times, also by the witnesses present that day in Slavyansk. Stopfake.org, a fact-checking organization from Ukraine, suspects that the story has been inspired by a motive from the famous fantasy TV show Game of Thrones.

The time of elections is especially vulnerable towards disinformation campaigns of any sort. Presidential elections are going to take place soon in Moldova and already the independent journalists in the country are trying to fight off a number of disinformation being spread about the candidate who will run against the current President. Interestingly, the narratives are very close to the ones spread about the Czech presidential candidate who ran against Miloš Zeman, the Czech president who defended his position in January 2018. Both candidates in the Czech Republic and Moldova have been accused of being too submissive to the West, and that they made secret deals with Germany or the European Union to accept refugees from the Middle East and Africa.

However, it would be a misconception to believe that only big disinformation cases like the crucified boy or disinformation campaigns leading up to and during elections are an issue. Disinformation narratives are also spread by more subtle messages, half-truths and manipulation are being spread continuously.

Ben Nimmo, an expert on information warfare, distinguished four main tactics of disinformation campaigns which are easy to understand and can be divided into the following clusters:

## Information warfare tactics

**Dismiss:** denying allegations or denigrating on the one who makes them
**Distort:** distort and twist the fact in order to serve your own narrative
**Distract:** durin away from your harmful activities by launching accusations elsewhere
**Dismay:** warn that anyone who oposes you will face disastrous consequences

After disinformation messages appear in the online space, they are easy to amplify by different tools on social media and elsewhere, often using fake accounts, which will be discussed in the following chapter. There is a lack of thorough, systematic and comparative research on the impact of disinformation. However, there are partial studies and data which should not avoid the attention of policy-makers.

### 1. 1. 1 In numbers

GLOBSEC Policy Institute revealed in its latest survey that many citizens from the Czech Republic, Slovakia, Poland and Hungary are inclined to believe some of the most famous conspiracy theories:

- 52% of Slovaks, 39% of Poles and 28% of Hungarians believe that Jews have too much power and secretly control many governments and institutions around the world.
- Majority of Slovak citizens believe that world events are not decided by publicly elected representatives, but secret groups that seek to establish a totalitarian world order.

The 89up researchers used data from Twitter, Facebook and other social media platforms to investigate the impact of Russian disinformation operations during the Brexit referendum. According to their findings, Russia Today and Sputnik, Russian state-media channels, produced anti-European posts on social media which were shared more than the posts of the official leave campaigns before the referendum took place.

Specifically, the anti-EU articles published by Kremlin-owned channels have 134 million potential impressions, in comparison with a total social reach of just 33 million and 11 million potential impressions for all content shared from the Vote Leave website and Leave. EU website respectively.

Furthermore, the total cost of the Kremlin media for the Leave campaign in the six months before the referendum was £1,353,000.

Russia Today and the Spanish-language version of Sputnik also increased their activity during the Catalan crisis in Spain, with the majority of their content supporting Catalan independence. Javier Lesaca from George Washington University analysed over 5 million messages on Twitter, Facebook and other social media platforms. Among other things, he investigated 100 social media accounts which were the most active in spreading news by RT and Sputnik. Out of the 100 accounts:

- 9 can be almost certainly classified as real accounts used by real people
- 7 were the official RT and Sputnik accounts on social networks
- 86 accounts cannot be assigned to any human being because they do not contain any original posts and show no signs of being used otherwise than to promote RT and Sputnik. Some of them post on average 1425 messages per day.

In 2016, the European Values Think-Tank, together with the statistical agency STEM, conducted a public survey exploring how many Czech citizens believe certain disinformation narratives and how much they trust alternative sources of information compared to traditional or public media. Amongst the findings are the following:

- 24.5% of respondents believe the alternative (disinformation, pro-Kremlin) media more than traditional ones.
- 38% of respondents think that the Ukrainian crisis was caused by the US and NATO.
- 30.6% of respondents believe that the fascist forces have a crucial influence on the Ukrainian government.

## 1. 2 Political interactions

### 1. 2. 1 High level policy makers

The disinformation campaigns themselves would be much less effective if they had not been multiplied and supported by other local proxies who further provided them legitimacy. The most effective ally which can help spread and legitimize disinformation campaigns is a high-level politician. Some of them might be victims of disinformation campaigns themselves, spreading them on their social media accounts or repeating the disinformation narratives to the media and the public, and in some cases this is done intentionally.

Furthermore, politicians can use disinformation media as platforms for spreading their own messages by giving them interviews or publishing their own articles, in the cases where the audience of such websites is attractive enough. However, by doing so, they provide disinformation channels legitimization that they would not otherwise receive, despite the fact that they do not abide by basic journalistic standards.

Adversaries can directly or indirectly financially support European politicians in rare cases. The closest example is the 9 million euro loan provided to the French far-right party Front National (FN) led by Marine Le Pen in 2014 by Russian banks. However, it has been argued that the primary favourite of the Russian Federation in the latest French presidential elections was François Fillon, a more mainstream candidate who originally had a better chance of winning the election.

For example, the expert on the relations between European far-right and Russia Anton Shekhovtsov believes that only after Mr. Fillon faced the accusations of employing family members in potentially non-existent jobs, Russia switched their focus to Le Pen.

More typical ways than direct and indirect financing is often connected to the Russian hybrid strategies, like media or diplomatic support. European politicians can defend Russian aggressive policies, lobby for Russian interests on the domestic and European level or calling for lifting the sanctions imposed on Russia by the European Union for the occupation of Crimea. In return, they get the attention of pro-Kremlin media, either from official ones or local proxies. They can be directly promoted by them, or disinformation campaigns can be employed to lessen the chances of other candidates during elections. Regular invitations to Moscow for official visits and meetings with their Russian counter-parts are also a common practice. Such visits then get a lot of attention by Russian media inside the Russian Federation, showing Russian citizens that the Kremlin and President Putin still have powerful friends in the West who recognize him as a powerful leader and an ally.

A good example is the non-traditionally good relations between the Kremlin and the Czech President Miloš Zeman. https://observer.com/2018/01/how-czech-president-milos-zeman-became-vladimir-putins-man/. Despite Mr. Zeman not having significant executive powers, he enjoys strong informal influence over some of the major policy-makers in the government and in Parliament. He often repeats disinformation and pro-Kremlin views, including his belief that there have been no Russian troops in Ukraine and that the conflict in Ukraine is a civil war – he never took this statement back even after Vladimir Putin himself admitted that they were present. His spokesperson regularly shares articles from conspiracy and pro-Kremlin websites including Sputnik on the official Twitter account.

The Czech President also surrounds himself with advisors and employees who have close ties to Russian business, for example Martin Nejedlý, who advises President Zeman on economic issues.

After spending several years doing business in Russia, Martin Nejedlý established a Czech branch of Russian energy company Lukoil Aviation Czech. His company received a fine for selling oil from strategic reserves, which was later paid by the Russian Lukoil headquarters so that Mr. Nejedlý could keep his position next to the president. Nejedlý has no security clearance and he does not have an official contract with the Presidential office, but he travels with Mr. Zeman on state visits.

### 1. 2. 2 Radical movements

Especially in the cases when it is not possible to reach out to mainstream and high-level politicians, the adversary can switch its focus to anti-establishment, radical, far-right or far-left groups and movements, or even paramilitary groups. There is no particular regard to their political affinity. Despite lacking significant influence in most European societies, radicals and extremists certainly contribute to the general unrest, chaos and distrust, which can be very useful for any actors attempting to use instruments of hybrid warfare.

The Political Capital Institute based in Budapest conducted research demonstrating the common ground between Russia and far-right parties in Central Europe. Amongst the most visible examples, they mention the Sixty-Four County Youth Movement in Hungary, an organization which recruits extremists inside and outside Hungary, stands out against Ukrainian territorial integrity and openly supports the so-called Donetsk People's Republic. Two members of the HVIM were even sentenced to 5 years in prison for an unsuccessful terrorist attack. The link between the Kremlin and HVIM is mostly ideological, unlike other Hungarian movements. Hungarian National Front 1989 (MNA1989) is an extremist movement which murdered a policeman in October 2016. The group has collaborated with officers of the Russian military intelligence agency GRU disguised as Russian diplomats on joint airsoft drills. Slovakia has experienced an increase of problems with new paramilitary groups. Members of some of them even travel to Eastern Ukraine to fight on the side of the Russia-supported separatists. Several individuals from Slovakia and the Czech Republic decided to do the same in the recent years. A group called Slovak Conscripts received training from former members of the Russian military intelligence special forces Spetsnaz. Czech far-right individuals involved in establishing the Czech paramilitary group National Home Guard conducted a public stunt which was very warmly presented in Russian-language media – they opened the so-called Donetsk People's Republic consulate in September 2016. The Ministry of Foreign Affairs of the Czech Republic distanced itself from the consulate immediately and the courts later ceased its activities.

The authors of the report claim that the quantity of direct and indirect links between far-right movements in Central Europe and Russian businessmen, politicians, diplomats and intelligence operatives suggest that they are all part of a broader effort by the Kremlin to undermine the region's stability in general and bilateral links with Ukraine in particular. Other evidence showing that far-right and anti-establishment groups or individuals in Central Europe do act in tandem with pro-Kremlin views was revealed after e-mails and social media conversations of Belarusian activist Alexander Usovsky were leaked. Usovsky established a fake non-governmental organization in Slovakia and managed to receive funding from Russian oligarch Konstantin Malofeev. The money was eventually transferred to the accounts of individuals in Poland, Czech Republic, Slovakia and Hungary with instructions to organizepro-Kremlin demonstrations.

## 1. 3 Economic operations

Business deals in strategic economic sectors can serve as a legal way to gain political influence, especially in cases of state actors using instruments of hybrid warfare against their adversaries. In Europe, the typical examples are energy deals with the Russian Federation and the ongoing negotiations with the Chinese People's Republic. Even though it is sometimes difficult to distinguish between reasonable and mutually beneficial business deals, there are experts especially from the security environment which look at any proposals to do business with Russian and Chinese state-owned companies with suspicion since they might pose important security risks and, in some cases, might also fulfil the goals of these authoritarian regimes at the expense of the interests of Western trading partners.

Chinese national projects like the One Belt, One Road are considered to be seeking not only economic development, but also advancing Chinese foreign policy objectives and spreading Beijing's political influence. Chinese state companies can even serve in assisting Chinese territorial claims in the South China Sea.

The Kremlin has been trying for many years now to increase the dependence of European countries on Russian energy. Its approach to making deals with European companies and governments has been questioned in many cases, lastly during the bilateral deal with Hungary on expanding the nuclear plant Paks II. Not only have the two friendly governments signed the agreement without any transparent and public tender as the EU norms require, the whole investigation on the matter has been highly non-transparent, raising suspicions that the reasons why the EU eventually approved the agreement were more political than technical.

# 2 Policy strategies

Create better conditions for journalists. Independent and investigative journalism should be supported, not limited by the government. Quality journalism is a building block of a resilient democratic system. Lack thereof gives more space to conspiracy theories and disinformation campaigns to be effective. Investigative journalists should have sufficient resources in order to be able to expose sources of disinformation and their motivation.

Establish investigative parliamentary committees. If there is a strong suspicion of foreign actors trying to interfere into domestic affairs, most of the parliaments in European countries have the competence to establish investigative committees to address these issues. They can conduct public hearings or request documents from the relevant actors.

Improve media literacy. Official state curriculums should take the phenomenon of disinformation into account and include media literacy programs. Students have to learn to distinguish disinformation from facts and get themselves oriented in the media environment. Furthermore, media literacy should be included in the university programs for future teachers.

Ensure transparent financing of political candidates. In many European countries, the current legislation is still not sufficient to prevent foreign financing of political parties or individual candidates. Either the existing rules are not implemented well, or adequate laws do not exist. These gaps in legislation can significantly simplify the process of covert support of favourable candidates during elections.

Send representation to relevant international institutions. On the European level, there are several institutions already focusing on researching or countering disinformation, including the EEAS East StratCom Task Force, the NATO Strategic Communication Centre of Excellence in Riga or The European Centre of Excellence for Countering Hybrid Threats in Helsinki. Participation in these bodies is purely voluntary. For example, in the EEAS East StratCom Task Force, there are only three team members dealing with pro-Russian disinformation, which is an extremely small force to counter the disinformation campaigns employed all over Europe.

Review the legal and regulatory tools. Non-transparent advertising on social media, spread of disinformation or fake accounts – all of these phenomena are possible due to the lack of efficient regulation of internet platforms. In some cases, there is no need to design new legislative measures, but proper implementation of media regulation can help ensure authentic content on the internet without breaching democratic principles. These methods have to be explored.

Invest into research. We desperately need more data on the impact of disinformation campaigns. Further research should be supported on this topic not only for the sake of academic advances, but also for the governments to understand its population, how it responds to disinformation and how it can affect their behaviour, including voting decisions.

Do not underestimate strategic communication. Relevant state bodies should have their own specialized units for strategic communication. They can produce fact-based and positive narratives about important issues, like the geopolitical base of the country and the importance of democratic values. They can also monitor the media space, reveal disinformation which have mobilizing potential.

# FAKE NEWS: COUNTERING DISINFORMATION

Péter Krekó
Senior affiliate at Political Capital Institute

The chapter is composed of three main parts. First, we take a look at the nature of disinformation and propaganda and examine how they spread. Analysis is conducted by focusing on the newest trends of disinformation, including both new operative methods and technological developments. The second part of the chapter deals with the importance of media literacy in a wider sense, as it is the alpha and omega of countering disinformation and hostile propaganda. The third and final part deals with possible countermeasures, by using an actor-oriented perspective, thus analysing, what individual, governments, journalists and NGO activities can do.

## 1 Tools

Disinformation is probably as old as humankind. Ever since people have waged war against each other, information elements have been present both in the wars and also related to them. Even Sun Tzu argued that all warfare is based on deception, and misleading the adversary has been present in most wars fought since then. State-operated, massive and detailed propaganda emerged before and during the First World War and was perfected by the totalitarian regimes of the 20th century. While the term information warfare is something relatively new, the concept itself is not new at all.

### 1. 1 Disinformation media

When addressing the role the media plays in spreading disinformation, it is crucially. important to distinguish between mainstream media and the so-called disinformation media. The main difference between the two is respect for the standards of professional journalism, such as objectivity, impartiality and unbiased used of sources, which mainstream media exercises. Meanwhile, disinformation media either ignores these standards, or in many cases, openly disrepsects or even misuses them.

As a result of this difference, mainstream media does not intentionally spread disinformation; mistakes and unintended inaccuracies may occur, but the general purpose of mainstream media is to inform the audience in a balanced and objective way. On the contrary, disinformation media intends to do exactly the opposite, and instead of objectively informing, it spreads one or more given narratives, and does so by openly disrespecting professional media standards. In other words, while spreading fake or inaccurate news is indeed a malfunction for mainstream media, for disinformation media it is a feature.

Another important factor is that though disinformation is often associated with various, obscure non-mainstream, alternative media channels, in fact there are certain countries where even mainstream media is often spreading disinformation. The most famous examples are the Russian state-operated RT and Sputnik, but in certain issues, related particularly to illegal migration, one may even mention the actions of Hungary's government-affiliated media conglomerate. Besides, one also needs to take into account the cases when high-ranking politicians get engaged in disinformation operations, spreading sometimes evidently untrue information in order to achieve their actual political objectives. One may recall, for example, Vladimir Putin's famous remarks in March 2014 that there were no Russian forces in Crimea, but Twitter-activities of U.S. President Donald Trump could also provide spectacular examples.

The problem posed by politicians and mainstream media channels spreading disinformation is that one cannot simply dismiss or ignore these channels as fake news, because their actions reflect the intentions and deeds of the given state behind them. Hence, in these cases the key to resilience is the awareness of the various manipulative techniques these channels and actors are using, which leads to the general question of media literacy.

## 1. 2 Social networks

What makes it important to address information warfare on social networks is the rapid technological development that has taken place in the recent decades. New technological achievements, including the rapid spread of social networks themselves, enable all actors exercising information warfare, either state or non-state, to have stronger, more sophisticated effects quicker than any time ever before in history. Hence, in order to properly address the question of countering contemporary disinformation, first the new trends and developments need to be examined.

Experiences of the alleged Russian intervention into the presidential election campaigns in the United States and in France in 2016 and 2017 respectively, demonstrate in practice that Russia often uses cyber means to gain data that could later be used for information warfare by employing social networks. In both cases, Russian-related hackers managed to get access to the servers of the candidate unfavourable for Moscow, and thereafter used the information gained to influence the election process, though with not decisive success. While the outcome turned out to be different in the U.S. than it was in France – mostly due to the well-prepared, smart counteractions of the staff of Emmanuel Macron – the trend itself has been clear: cyber actions are often used to enable future information operations.

Besides, as pointed out by Péter Krekó, Political Capital's executive director, artificial intelligence can also generate content, which is why Russia and China are focusing on AI-research, and Putin even claimed that the great power who wins the competition for being the leader in AI technologies will rule the

world. This technology allows anything to look real, and if everything can be real or fake, objective facts would disappear - this is why the technology could be a huge threat. MPs from the UK House of Commons were also warned by Edward Lucas, the senior VP of the Centre for European Policy Analysis, about the dangers of this technology, and that the country is not ready to defend itself against these threats.

### 1. 2. 1 Bots and botnets

A particularly important aspect of how disinformation is supported by cyber means is the use of automated accounts, so-called bots to spread and amplify disinformation. A bot is a software that is being used; in the context of social media, bots are fake social media accounts controlled by organisations or governments aiming to influence online discussions; they generate a variety of content on online – this includes harmless, and harmful ones as well. For instance, Twitter bots can be set to retweet given hashtags or words in large quantities, while Reddit bots can be instructed to downvote or upvote views disagreeing with it – which is useful because downvoted comments and responses are hidden by Reddit. In this regard, this technology allows hostile actors to amplify manipulative information on social media and steer discussions towards views favourable to them.

As botnets are relatively easy to detect based on their inhumanly high level of activity and monotonous work, recently a new type of them emerged, the so-called cyborgs. Cyborgs are such botnets on Twitter and other social media networks, into which occasionally also a human operator writes content. Cyborgs are a lot harder to detect by automated filtering mechanisms.

### 1. 2. 2 Trolls

As opposed to bots, trolls are humans using fake social media accounts to provoke others on these platforms and support hostile actors' goals through aggressive communication. According to a report by NATO StratCom, there are two types of trolls: classic trolls who seek to cause emotional harm without any ideological connections, and hybrid trolls who disseminate disinformation and conspiracy theories. Often, hybrid trolls are employed by someone specifically to disrupt online conversations; a good example for this is Russia's Internet Research Agency in St. Petersburg, where employees are paid to run fake blogs and spread disinformation in social media comments. According to NATO's StratCom Centre of Excellence, the traditional modus operandi of Russian trolls are built on the cycle of luring, taking the bait and hauling in. This involves one troll posting a controversial, topical comment to generate attention and provoke a response. The trolls wait for someone to formulate opposing views or even post opposing views and exaggerations to lure a non-troll into the conversation. Afterwards, trolls post content deviating from the topic and make the discussion antagonistic, while creating the impression of a discussion involving various differing views on a range of

topics. This way, hybrid trolls legitimise and promote the viewpoints of hostile actors, while discrediting the credibility and stability of its targets.

The NATO StratCom CoE found five troll types: blame the US conspiracy trolls that aim to encourage distrust; bikini trolls – accounts with attractive profile pictures – to engage with targets; aggressive trolls to coerce people into leaving conversations; Wikipedia trolls that edit pages in a way beneficial to the Kremlin; and attachment trolls that link pro-Kremlin content. Chatham House believes that trolls are sometimes used as decoys. They are essentially flooding the online space with comments, which then have to be moderated – this serves the purpose of wearing down the other side. Another document published by Chatham House suggests that trolls have created Twitter accounts (@Vaalit on Twitter) that look innocent and even official, whose posts some people consider to be official – but in fact they spread pro-Russian disinformation.

Considering the fact that trolls are human users, it is harder to recognise them than it is bots. In fact, it is an increasingly tough task to recognise Russian trolls due to the fact that propaganda efforts are becoming increasingly sophisticated. They regularly post pro-Kremlin content or comments favouring pro-Russian politicians, use incorrect grammar/spelling, have only few followers, alternative sources and are obsessed with certain topics. An academic study found that trolls ‚tend to make more inflammatory posts," are more likely to swear, use positive words less, and are less likely to use conciliatory language (could, perhaps, consider). Trolls also try and succeed in engaging people in discussions, which means that they post more in a given comment chain than normal users.

### 1. 2. 3 Deepfakes

Deepfakes are computer-generated fake videos and audio records that look very real. To create such a video, an actor sits in front of the camera and speaks, while a computer generates the same expressions in real time on an existing video of another. This means that, you can literally put into a person's mouth anything you want. There are methods available to generate human voice samples and even realistic photos. Experts say that it is unlikely that social media companies are ready for handling the deepfake problem. However, it must be mentioned, that the technology still encounters issues: there are odd frames in deepfakes videos, some of the frames look blurry and it's all a bit clunky. However, the technology is developing every day, and it can be one of the main threats to democracies in the future.

### 1. 2. 4 Social bubbles

News consumers, especially young citizens, are turning more and more to online platforms (including social media) and messaging to inform themselves about political events. The way online search engines and the algorithms of social media sites work might filter bubbles. Many, but not all, engines are designed to recommend

news to online users, prioritise like-minded content and content that conforms to already existing preferences. These algorithms have the potential to create an environment in which news consumers are not subjected to counter-attitudinal information, an echo-chamber that reinforces what people already believe in. These phenomena can help polarise societies further, fragment the public sphere and even create new divisions in societies.

Some studies suggest that in certain European countries the filter bubble problem is much less pronounced. The Council of Europe also emphasised that strong and independent public service broadcasting is especially important in countries with highly polarised societies, where the proliferation of one-sided information or outright disinformation is amplified by social media.

In addition, the combination of algorithms and human factors is the reason why social media content containing misinformation is able to spread faster than factual ones. Facebook, Twitter and YouTube are all based on deep learning algorithms that prioritise content with more engagements; and these methods also take into account that people are more likely to keep using social media if they see content that has already received numerous likes, retweets, etc. The human factor in this issue is that people are more likely to react to content playing on existing fears or biases, so inflammatory tweets will generate quick engagement. Afterwards, the technical side takes over: after a Tweet – for instance – is retweeted, favourited, etc. the algorithms show it to more users, which will generate even more engagement. Then, this circle repeats itself.

## 1. 3 Useful idiots

Disinformation in most cases is built on the lack of knowledge and awareness of the targeted audience, and sometimes the explicit credulity of it, depending mostly on its general values and preferences. These two factors, the general lack of awareness and the readiness to believe things too easily, constitute key vulnerabilities in the fight against disinformation.

The so-called useful idiots are those individuals who voluntarily spread and amplify the narratives promoted by disinformation channels. Their motivations may vary, ranging from political, religious or identity-related convictions to various forms and anger, frustration, affection and conspiracy theories, or simply the will to attract extra attention.

The effect is, however, common: narratives, fake news and distorted information gets spread by these actors. This, besides the evident amplification effect, add also to the overall credibility of the given manipulated narrative, due to two main reasons. First, the useful idiot is in most cases is not related to the state or non-state actors behind the given piece of disinformation. Hence, they are able to spread the news and information which they really consider to be true, under the umbrella of referring to – and, in most cases, rightly

so - the freedom of speech, thought and conscience. Second, as useful idiots are honestly convinced about their own truth, they are a lot more committed to spread their own story than paid, professional trolls and other information agents. The fundamental importance of these values makes it a lot harder to step up against the useful idiots than against known, professional information agents.

The so-called useful idiots may pose particular threats if they hold important political, public, business or technological positions, thus their influence gets strengthened by the power of their position.

## 2 Media literacy

As disinformation in the media is based on misusing all aspects of how media channels work, increasing media literacy of the society plays a key role in increasing the overall social resilience to disinformation. Format and content of these education activities needs to get tailored specifically for the target audience.

### Media Literacy Guide:

1 Verify the credibility of the source of information
(editorial address, ownership, method, financing)
Disinformation portals are non-transparent
and generally do not provide the such information.

2 Read the full article, not just the caption and the first paragraph

3 Verify the identity of the author
The authors of disinformation articles are generally anonymous.

4 Pay attention to the language and text level
The misinformation articles are typical of vulgarisms, misspellings
and the overall low level of language and text itself.

5 Check the release date
Disinformation sites often recycle articles or photos.

6 Search for quoted sources
Check the quoted experts if the text points to another resource, locate it.

7 Verify with other sources
Do not use just one source of information but crosscheck
each information with other sources.

## 2. 1 Education of the public

Particular attention needs to be paid to the training of journalists. This is the key importance of journalists as producers and providers of news. Journalists and newspapers serve as the primary source of information for the general public, which is a double-edged sword in the struggle against disinformation. Conscious, well-trained journalists are the best tools of combatting fake news and hostile disinformation; while if things go wrong, journalists might serve as the amplifiers of the faked, doctored, manipulated narratives as well.

Besides training journalists, also widespread education programs are necessary for the wider public, starting preferably already with school education. Media literacy and consciousness should be an integral part of the school curricula.

## 2. 2 Recognising fake news

When it comes to content of media literacy education programs and projects, the key element is to recognize if one is faced with a disinformation media channel. As demonstrated above, disinformation is often spread via non-mainstream channels that are often collectively referred to as alternative media, composed of thousands of websites and social media pages operating in several languages. In fact, most of these so-called disinformation channels are relatively easy to recognize, even by non-specialist everyday users. It is also possible to identify falsified, faked or doctored pictures. The Ukrainian NGO Stopfake that has been engaged in countering Russian disinformation since 2014, released guidelines for how to recognize fake pictures and doctored videos. Google has also published detailed guidelines for recognizing misused pictures by relying on reverse image search.

All in all, the knowledge is already available on how to distinguish reliable sources of information from fake news channels. It is hard to achieve 100% accuracy and filter out all fake news and anipulated information, however, increasing the resilience to them is indeed possible even on the individual level.

Mastering these skills and practices is particularly important, because technological development may easily go so far that people will have to live in a world where every piece of information can be fabricated. Sloppy articles, unprofessional websites and easily recognizable trolls will be replaced by far more diverse and more sophisticated content. Deepfakes, described in the first part, are just one example, but many others may come in the very near future. Among such circumstances emerging, it is crucially important to lay down the foundations of media literacy and resilience to information pressure well in advance.

# 3 Preventing spread

Globalization and the rapid development of internet-based communication have transformed how people get the news. According to a PEW survey conducted in 2016, about

40 per cent of all Americans already get most of their news online; the younger a person is, the higher the share of online media in their news consumption is, meaning that the importance of online media will only grow over time.

## 3. 1 Politicians

Politicians and governments have a key role in countering disinformation, originating from their power to shape the legal environment in which both disinformation and its countermeasures to it have to operate. In other words, politicians and governments are the ones who shape the playing field from the legal perspective, and partially also from the economic perspective.

As a general rule of how politicians and governments may act against disinformation, analysing past mistakes and learning from them is a useful and efficient practice. By using particular examples of earlier cases of successful disinformation operations might well help the audience understand how such threats work, and how it is possible to counter them. As the threat Western countries are facing shows considerable similarities, there is great potential in international cooperation for increasing the media and information literacy of the society. Sweden, Norway and Finland are already engaged in such a cooperative project, the European Union is also supporting such actions, and so are many national governments.

### 3. 1. 1 Pressuring big players

The most important tool of counteracting disinformation could be legal and administrative measures taken by governments and politicians, aimed at making internet and social media companies more engaged in actively countering the spread of disinformation and hate speech on their platforms. Experience already demonstrated that the elaboration of such measures is a lot more effective if conducted in close cooperation with journalists and the civil society. Governments, tech companies as well as actors in civil society shall work together to create functioning and actionable policies of identifying and taking down accounts spreading such content, as well as supporting fact-checking activities, and jointly increase media literacy.

Social media companies play the largest role in combatting the presence of bots and trolls online. Both Twitter and Facebook started removing fake accounts from their sites, which can be considered a good first step. However, social media could do more, either by itself, or motivated by governmental measures and perhaps also by social pressure. For instance, the sites could be required to restrict the visibility of trending misinformation and to find a way to remove misinformation from trending searches – for example by employing editorial teams – to stop the circle of engagement.

Governments and politicians have a crucial role in countering fake news portals that are motivated not by political issues, but simply by the willingness to earn money.

Good examples for this type of fake news portals are the disinformation clickbait websites that operated in Veles, Macedonia during the U.S. presidential election campaign in 2016. One needs to recognize that the difference in motivation does not decrease the risks posed by activities of these websites, as they might still significantly distort public discourse, as exactly the Macedonian websites demonstrated.

### 3. 1. 2 Crisis communication

Disinformation may cause the most harm if it succeeds to falsify or distort messages of national governments, individual politicians, international organizations, as well as of major business companies. Disinformation attacks may be highly diverse, ranging from spreading outright lies and using sophisticated forgeries, to online smear campaigns and hacking.

Hence, it is of crucial importance particularly for the political actors, but also for business companies to have a secure and trusted communication channel through which they can communicate with each other and can deliver their messages and narratives if a disinformation-related (or other) crisis happens. As establishing such a channel and building up trust takes significant time, actions have to be started well in advance as a general precautionary measure.

### 3. 1. 3 Other measures

Governments also have the power to adopt laws and regulations that limit, or even sanction the spread of fake news and disinformation. Such measures may include fining media channels for spreading disinformation. Ofcom, for instance, has issued multiple rulings condemning RT for significant failings in its broadcasting, and RT was thus forced to publish multiple corrections. In some countries administrative measures may even include the banning of foreign media channels if the local government deems it necessary; for example, Ukraine banned several Russian-language media channels by claiming that they spread disinformation, which posed a security risk in the context of the ongoing armed conflict in Eastern-Ukraine.

Administrative measures will probably play a key role in countering deepfakes. One possibility to negate, or at least mitigate the dangers posed by politically motivated deepfake videos, is to establish administrative double-checking and verification mechanisms. For example, every speech made by state leaders must immediately be published in writing, thus a possible deepfake distorting the video record of the given speech can be countered by pointing to the written version of the text. Another, possibility is to legally sanction the production of deepfake videos, based on copyright infringement, defamation or violation of privacy. Of course, the legal environment necessary for such actions can be established only by states, meaning that states are likely to keep playing a key role in countering deepfakes.

# GUIDE TO SURVIVE IN CYBER SPACE

Alexery Yankowski
IT Strategy and Cybersecurity consultant

When we are talking about countering fake news, we should realize that we are most likely acting against a powerful enemy - state actors, that control state cyber combat forces or state-sponsored professional hacker groups.

These are professional organizations and organized crime groups, that have unlimited resources and time. They are principally different from the enemies that we faced 15 years ago, comprising mostly talented individuals like Kevin Mitnick, a convicted hacker who is now working as a security consultant among other for the FBI or from security consultants, whose time is limited by the time of the project. Enemies we face are mature organizations with project managers, and professionals that specialize in certain areas of cyber activities. One would do the initial compromise, the others would do elevation of access, still the others would be experts in the business that you operate, knowledgeable of when and how to hit in order to generate the largest amount of damage.

Most things on the Internet can be hacked. If they want to target you, they will most likely be able to do so – it is a matter of time and money. It does not mean that we have to give up, though. We want to make intruders' life difficult, and increase the price that needs to be aid for compromising your privacy. Also, if you protect your things properly, you may win the time, which may be necessary to physically secure yourself, or to achieve your mission, such as publishing the information.

I provide advice as to how to protect against different types of attacks. When using this guide, you should first of all use your judgement in deciding as to how to act. Technologies evolve very fast, new threats and countermeasures arise every day, and you should realize that this guide may become outdated by the time it is written.

Through the document, we attempt to provide links to the resources that should be frequently visited to obtain up-to-date information. By no means is the provided advice, the list of tools and links exhaustive. Its purpose is to increase your awareness, and provide you with a direction. There are more comprehensive guides out there, and the goal of this document is to collect the most important things in one place. The best way to achieve protection is to hire cyber security professionals to take care of your digital assets.

Before an attack is launched, intruders may collect detailed profile on you, your habits and behavior using social networks, and public info they find about you on the Internet. After attackers get a hold of your PC, they install monitoring software that sends all information about what you do on your device to a remote control center, operated by hackers. They can also change information on your PC, intercept keystrokes, passwords and your digital keys.

## Attack scenarios

Eavesdropping on your communication by getting control of your devices, or intercepting communication at your service providers' networks;

Disseminating fake news on your behalf, by stealing your digital identify – getting control of your social network and public blog accounts;

Attacking your finance and personal lives – by hacking into your home devices, spying on your movements, stealing money from your accounts, and attacking those closest to you, including your children;

Threatening to disclose your personal data or confidential information;

Attacking via your colleagues, via an organization your work for, or a someone you trust, such as a software or a hardware supplier;

Encrypting your data and demanding a ransom to decrypt it;

Misusing computing resources of your device, for example, using it for mining cryptocurrencies;

Physically stealing or confiscating your equipment;

Infecting device, when you open a legitimate-looking email that contains infected attachment (the most common way);

Attacking your PC via vulnerability in software installed on it;

Access they gained can be used to:

- spy on you and everything that you do on your device;
- issue payments on your behalf (if they steal your Internet banking passwords/keys);
- attack others from your computer;
- send or post fake information on your behalf;
- encrypt all your files and require you to pay ransom;

It is typical for attackers to monitor for months, and wait for the right time to attack in order to architecture success.

# 1 Protection

Based on your professional activities, you should understand which organization or country is your enemy. This may provide you with a better understanding of what means and tools that are likely to use in order to get a hold of your information.

Threats may vary from a government request to the internet provider or a cloud service provider to provide your data, to actually hacking into your or your employer's computer systems and phones, or bribing an employee of an operator. In some countries, journalists may be physically threatened and followed based on their professional activities. A situation when one is taking part in protests, getting into territories controlled by terrorists, or crossing state borders may also have specific threats and safeguards. Your current situation may impact such decisions as:

- whether or not to have a separate PC and mobile phone for personal and professional use;
- which provider and jurisdiction to use to store your confidential data and e-mail;
- whether to use encryption, which tools to use;
- how much to post on the internet, and whether to be on the internet at all;

It should be understood that most things on the Internet are being logged, and may be obtained with or without a court order by authorities, or by hacker groups, supporting hostile governments. Even if you do not use the Internet at all, your exact location, history and time of your phone calls is known and recorded by mobile service operators, and can be provided to third parties, for example, by a bribed employee.

You may be surprised to see history of your daily movements and exact locations you visited many years ago, when you started using google map, for example.

A history of your phone calls and your e-mail messages (so-called ‚metadata") are likely kept by your service providers, and will be given to authorities requesting it without the court order in many jurisdictions. And the metadata can provide a whole lot of information about you and your activities.

Despite the fact that your profession most likely requires you to constantly be on the Internet, you may want to limit your participation in the social networks, the amount of information you post about yourself, your location, etc., possibly use a separate account which is not linked to your personal account, or even not to be on the Internet at all.

It is also recommended to limit use of the location services and disable history in various online services, as described in the subsequent sections of the document. Despite the most restrictive privacy policies of most service providers, the data that they have about you may be stolen by hackers.

## 1. 1. Defense-in-depth

Defense-in-depth is one of the key concepts of cybersecurity. The security concept itself was developed by the Roman military more than two thousand years ago. It is the practice of layering defenses to provide added protection. Defense-in-depth increases security by raising the effort needed in an attack.

This strategy places multiple barriers between an attacker and an enterprise's computing and information resources." (ISACA). Romans have been building castles inside other castles, so when the outer castle has fallen, the enemy has to defeat the inner one.

From a cybersecurity standpoint, it means that you need to build as many barriers for your enemy as possible and protect your most valued assets with even additional barriers. In practical terms, it means that you should use as many layers of safeguards as possible. For example, in addition to standard mechanisms such as antivirus, two-factor authentication, hardened computers, etc. you may use additional encryption to protect your most sensitive data, or consider using separate equipment, disconnected from the Internet, to handle your most sensitive information and projects.

The security of your information is also as strong as the security of your weakest link in a set of services you are using. I have seen an example when a company used very comprehensive and expensive security tools, yet its infrastructure was compromised due to a weak password of one of the system administrators, used in the online service.

Although, in an ideal world security works seamlessly, this is rather true in the case of large mature corporations, or for individuals that want to achieve a standard level of protection. In reality, the more security you need, the more inconveniences you may be facing. Using strong passwords, additional protection tools, sometimes separate accounts, computer and phone may cause additional complexity and inconvenience. You should be ready for this.

When it comes to the most sensitive data, it is recommended that you limit the control of individuals or organizations. The data can be exposed at work, at your service provider, or even at home. In case you use third-party services (your employer, or a cloud provider) to store your data, you should at least encrypt it. Try not to share a computer with sensitive data with anyone, including your family. Make backups of sensitive files on an encrypted USB drive.

Tools and systems provided in an open source form are generally considered more secure, since chances are that the security bugs and possibly backdoors have been minimized by a large number of members of the on-line development community that develops the system and reviews the source code. When installing at open-source solution, look at the history and reputation of the group that developed it, track record of identified and resolved security vulnerabilities. Download the tool from the original vendor's web site, verify MD5 checksum or digital signature of the software before installation, and often check for updates.

In contrast, software that is provided without a source code is a black box, and you are trusting your security to its vendor. It may contain hidden security vulnerabilities or even backdoors to let the 3rd parties in.

# 2 Buying a computer

For regular computer users, from the standpoint of security there is not much difference, whether to use Intel-based PC with Microsoft Windows, or a Mac.

**Use a separate computer for the most sensitive tasks**. You may want to consider using two computers - one to work with sensitive information (with minimal exposure to Internet), and thesecond one - for your regular activities, including email and web browsing. You should minimize the amount of software installed, and the amount of activities you perform on a secure computer.

**Use a separate digital identity to work with sensitive info**. Use a separate set of Internet accounts to work with the most sensitive info. The two sets of accounts (the one that you use for normal work, and the one that you use to work with the sensitive info) should be completely disconnected from each other.

**Use pre-2013 computer, under Linux or FreeBSD or OpenBSD**. If you are working with highly sensitive information, you may consider using an old (pre-2013) computer without AMT functionality. It is recommended to reinstall it and load it with Linux or FreeBSD operating system. When you do this, it is also recommended to replace BIOS (which may contain backdoors) with BIOS from Libreroot www.libreboot.org.

**Custom-build or order a secure PC**. As an alternative to using old equipment, you may consider custom-building or ordering a secure computer without the AMT functionality, with pre-installed Libre-root BIOS and a secure Linux, such as this one: www.minifree.org.

## 2. 1 Protecting a computer

Install commercial antivirus or endpoint protection solution that provides regular updates. This software shall protect data on your hard disks, scan your email as well as your browser sessions for threats.

Regularly apply security patches and keep your software up-to-date at all times.

Activate built-in security features, such as host-based firewall, to disable incoming connections to your PC.

Harden your operating system. This includes disabling unnecessary services, unnecessary disk shares, and implementing a variety of strict configuration settings.

Encrypt hard drive of your PC and sensitive data. On Microsoft windows this can be done using Microsoft Bitlocker solution.

Alternatively, you can use PGP Desktop or a similar tool. This type of encryption only protects your data when your PC is turned off. It is primarily designed to protect the data in case your computer is lost or stolen.

It is recommended to encrypt sensitive files on the disk of your computer with additional tools.

Backup sensitive data. All critical data should be backed up on external media, preferably in encrypted form. In case a cloud is used, the data should be encrypted as well.

Install special software to securely remove files. Beware that your files are never permanently deleted from your hard disk, and can be easily recovered by someone having control of your computer, unless you use special software for file deletion. It is recommended to install such a software to perform secure file deletion (for example www.bleachbit.org ). It should be noted, that data from SSD disks (and from the USB-sticks) cannot be easily deleted, even with help of such a software.

Minimize the amount of third party software installed on your system. Every piece of additional software you install could potentially contain a backdoor or vulnerability, and increases the risk of compromise to your system.

Make sure that any third-party software you install has a valid digital signature. In case you install any third-party software, make sure that is digitally signed, and the signer's certificate is valid and trusted. More information can be found here: www.samlogic.net/articles/code-signing.htm

Secure behaviour. You should understand though, that antivirus software only protects from known attacks, it is not a panacea against so-called zero-day attacks, or new malware that may be crafted by hackers specifically to target you. You should use caution opening email attachments and browsing the Internet, as described in subsequent sections. You should not download and run software from unknown sources, trust self-signed certificates or pieces of software code.

# 3 Email security

Phishing is a type of social-engineering attack, and one of the most common ways of breaking into computer systems today. It comprises of sending a legitimately-looking email to a person, encouraging him or her to open an infected attachment that runs a malicious code that allows an attacker to take control over end-user's device. Phishing may also fool a person to click on a link to an infected website, or disclose his confidential information, such as passwords, credit card numbers, etc.

Variants of phishing include sending SMS or instant messages (so-called wishing), or placing phone calls to the victims.

It is extremely important to be able to recognize a phishing letter. The problem with this is that phishing attacks are constantly evolving. Nowadays, a phishing letter may be accompanied by a phone call from a trusted counterparty, made in connection to the phishing letter, encouraging a victim to open this letter. For example, a journalist may receive a call from a person who wishes to publish an urgent and important evidence, to be provided in the attachment of the email message.

It is important to understand, that the source email address of the letter you receive can be easily forged, and the letter may seem to be coming from your boss at work, your friend, or someone you know and trust.

The links provided in the letter may look like links to the legitimate sites, but may hide links to the compromised ones. To check the link, you should put the mouse over it, and most browsers will display the actual address that hides behind the link. Use a third-party service, such as www.scanurl.net.

## Phishing letter

Unsolicited, from someone you do not expect to write you;

Creates a sense of urgency, and encourages you to quickly open an attachment or click on a link provided in the message;

Seems to come from a very trustworthy source, such as a government agency, or a regulatory body;

Contains misspellings or other irregularities (such as missing corporate logos, signature and contact information at the end, etc.). Obviously, well-prepared campaigns will not have that;

Suspicious to you, for example. the tone of the letter seems unusual;

Encourages to provide your password, PIN-code, CVV, or personal info;

It is important to understand, that the source email address of the letter you receive can be easily forged, and the letter may seem to be coming from your boss at work, your friend, or someone you know and trust.

The links provided in the letter may look like links to the legitimate sites, but may hide links to the compromised ones. To check the link, you should put the mouse over it, and most browsers will display the actual address that hides behind the link. Use a third-party service, such as www.scanurl.net to check if the link is safe.

You can also use third-party virus scanners to check a potentially infected attachment, however, you should be aware that the content of this attachment will be made public by the virus scanner provider.

When you send your message to someone, it can be intercepted and read at the following locations:

- at the computer of the sender and recipient;
- at your internet router at your home;
- someone connected to your Wi-Fi;
- your internet service provider ;
- any network providers in between you and recipient of your message;
- your email provider in case you maintain your mailbox with him;
- hackers or government authorities that gained control of any of the above;

A number of measures should be used against this including email encryption, choosing the mail provider and jurisdiction that is right for you, and properly protecting your device.

When choosing your email provider, you should consider criteria such as a jurisdiction, where this provider and its data centers are located, how cooperative and privacy-conscious that provider, whether there is a ‚rule of law in the country, whether local laws protect individuals from potential misuse of power, whether the ‚proportionality principle" is followed, whether there is a legal assistance treaty in place with the country where your enemy is located, etc. Some jurisdictions provide better protection from misuse of power by authorities than others. You should consider an independent analysis, such as www.thatoneprivacysite.net/email-comparison-chart.

For example, provider Protonmail is based in Switzerland, which is known for good protection against potential misuse of power. There may be pluses and minuses of different locations, depending upon who is your enemy.

After you install the software, you will need to generate a pair of keys, and exchange public keys with your counterparty. It is recommended to keep your private key on an external drive to decrease the risk of theft of your private key. Consider reading an encryption tutorial www.bcu.ac.uk/Download/Asset/3384b399-3911-e611-80c7-0050568319fd and an OpenPGP user guide www.pitt.edu/~poole/PGP.htm.
Electronic Frontier Foundation provides step-by-step instructions as to how to set up GnuPG, Thunderbird and Enigmail, in order to use Thunderbird email client with encryption https://ssd.eff.org/en/module/how-use-pgp-windows.

You may consider using a third-party software in order to exchange encrypted and digitally signed email messages with your counterparties. PGP (Pretty Good Privacy) is one of the oldest encryption programs developed for individuals in the beginning of 90th.

Currently PGP is part of Symantec. However, OpenPGP - an open source publically-available implementations is available for various operating systems and mobile platforms: www.openpgp.org/software

You should be aware that even if you sign and encrypt your messages, the email address of the sender, recipient, subject and time of sending message will still be unencrypted.

## How to treat suspicious emails:

Don't open attachments, click on the links or run any programs attached;

Try to contact the sender of the message and ask him whether he has really sent this email to you;
Don't provide your personal info, passwords, PIN-numbers, etc.;

If the message is from the bank (or other trusted authority), encouraging you to click on the clink to access your internet banking application;

Do not follow the link in the message. Instead, follow your usual steps to access the application;

# 4 Calls and messages

Your phone calls can be intercepted at the following places:

- in the room where you are located;
- on the phone itself, in case it has spyware program installed on it;
- between you and your mobile operator
- at the mobile operator's network;
- on the way to your counterparty, by his operator's network or on his device;

Since mobile calls can generally be intercepted, it is recommended to make secure voice calls through messengers that support encryption and work over the Internet (which could be your mobile provider's Internet or a separate internet connection). Most popular messengers today support placing encrypted voice and video calls between users using ZRTP protocol that allows using a one-time cryptographic key for each session. Before starting communication, you should verify the digital key of your counterparty, in order to avoid a man-in-the middle attack. Step-by step instructions for WhatsApp and Signal messengers are available here:
www.ssd.eff.org/en/module/how-use-signal-android
www.ssd.eff.org/en/module/how-use-whatsapp-ios .

Minimize a number of third party apps. As with the computer, you should minimize installation of third-party applications on your mobile device, since each application could potentially have a backdoor, an undocumented functionality or a vulnerability that would allow intruders to spy on you.

Minimize permissions of third party apps when you install them. If you decide to install a third party app, check the number of downloads of the application (how many downloads are there, what other users write about the app, what is the rating), information about developed (what other app he developed, whether this is a well-know company, etc.) During installation, provide very minimal necessary permissions to the app (for example, consider whether giving access to your camera, contacts, documents and storage, microphone, etc. is really necessary for work of the application).

Do not use jailbreak on your iPhone. Jailbreaking brings a number of security consequences.

Do not download software from outside of the App Store or Google Play Market. Chances are higher that you will download a hostile application with a backdoor.
Encrypt your phone. You can use built-in features for that. Use strong password for encrypting your phone.

Configure device wipe after failed logins. Remember, that if you do that - your data will be lost, unless you had a backup.

Make a well-informed decision whether you want to backup all your data in the cloud. The cloud provider will have access to your data, as well as others who get control over it.
Set up a strong password. Set a strong password for phone encryption and for accessing the phone.

Disable services through which you could potentially be attacked. Disable AirDrop services (in iPhone), bluetooth, or Internet hotspot on your telephone.
Consider disabling fingerprint authentication under certain circumstances. You may also consider disabling authentication by fingerprint, in case there is a risk that you may be physically detained.

As it is recommended to use a separate PC to handle most confidential documents and email, it is also recommended to use a separate phone to handle the most sensitive information. This phone should be hardened by configuring the strongest security settings (or a special version of an operating system), and should have a minimal set of security tools (such as VPN, secure messengers, encryption tools, etc.) installed.

If you are attending a public protest, or a zone of a military conflict, you may consider using a burner phone - an inexpensive or an old phone,

which you will use to accomplish your mission and then can throw away, or which you can easily give up in case you are detained. Such device should have a minimal amount of information on it.

As with any service provider, you should read carefully the privacy statement of the provider of your messenger services. It is also preferred to use open-source messengers, such as Signal or SilentPhone.

Enable two-step verification for your account, for registering your phone number again with the messenger.

Configure privacy and security settings. Disable live location, enable security notifications (to see notification when our contact's security code has changed), disable collection of your activity data aimed to improve product performance, consider changing other settings in accordance with your preferences (for example you may wish to consider whether to let others see if you are online, etc.).

Disable storage backup of your messenger in the cloud. Since the backup is stored unencrypted, the service provider (or other who gain control of its infrastructure) will be able to see the content of your messages.

## 5 Web browsing

Use SSL to work with web sites. Whenever possible, use SSL to access web sites. Ensure there is https:// (not http://) in the site URL address. Remember, that all your traffic can be eavesdropped, if SSL is not used.

Don't work with sites that have invalid certificate. Look for warning messages from your web browser about web site's certificate being invalid. For Chrome, for example, make sure that a little lock next to the web site's URL is not red, as displayed below.

If you see this message while accessing a site that you regularly visit, it could also mean that someone is intercepting your connection to this site, and can see all your traffic. This may often happen in the hotels or some public places.

Spot fake websites. Carefully examine the domain name of the web site. Sometimes hackers create sites, that look like legitimate web sites. For example, they could create a site that looks like your Internet banking application, your favorite online store or PayPal, and encourage you to enter your password there. Or they could masquerade as a site like Microsoft or Gmail. Always look at the domain name and make sure it is a genuine one. For example, a fake domain for Gmail could look like the following: gmail-c.com or gmai1.com - that resembles the actual site. Also look at the graphics of the web site, logos, and spelling errors.

Don't cache passwords and credit card numbers in your browser. Do not store passwords of your critical applications and credit cards the in the web browser.

Keep the version of web browser up-to-date and install security patches on time.

Minimize the number of third-party plugins. Plugins are third party programs that you can install on the top of your browser to add additional functions or improve your browser experience. As with any third party programs, plugins could potentially contain unwanted components, and spy on you. It is recommended to minimize the number of third-party plugins installed, or not use them at all.

Websites that you visit use multiple ways of tracking your activity, primarily cookies. You may want to disable the use of cookies on your web browser. You can also install a special anti-tracking software, such as Privacy badger www.eff.org/privacybadger/faq. However, you can still be tracked by IP address.

In order to increase the level of anonymity, use different types of anonymizer tools for web browsing. This could be:

Encrypted proxies. Proxy is an intermediate computer on the Internet that your web browser connects to before connecting to the destination site. A list of some encrypted proxies can be found here:
www.techradar.com/news/the-best-free-proxy-services-of-2018

VPN service. In contrast to an encrypted proxy that encrypts traffic from your web browser, a VPN encrypts all traffic from your device., www.thebestvpn.com/. You would need to install and run VPN software on your device to use this service. VPN comparison charts:
www.thatoneprivacysite.net/vpn-comparison-chart/

Tor browser. Tor network provides online anonymity. It is a global distributed network, run by volunteers, designated to protect against surveillance, and also to circumvent online censorship. Tor browser that you install on your device connects to Tor network, then your traffic is routed within this network via unknown paths, until it gets to the destination site. More information about Tor network can be found here: www.torproject.org/. You can download and install Tor browser for your computer or a mobile device (preferable from the link provided above).

The above solutions only encrypt your traffic between your device (or your web browser) and a provider of the VPN or a Proxy service, or from your browser to the Tor network. Tor is the best way to achieve anonymity, however it also does not guarantee full protection.

To facilitate anonymity, it is recommended that you also use a separate secure operating system, and a separate set of accounts. Resources to test whether your browser protects you from tracking:

www.panopticlick.eff.org/. Resource to check whether you have a DNS leak that allows to trace you to find out your Internet Provider:
www.dnsleaktest.com/

## 5. 1 Use of public Wi-Fi

You should realize that when you use a public Wi-Fi hotspot, the provider of the Wi-Fi network could monitor your network traffic, and see what sites you are connecting to. If you do not use encryption, the provider will also be able to see the content of your traffic. Your computer can also be attacked by other devices, which are connected to this public Wi-Fi.

Use anonymizers. It is recommended to use the same set of anonymizer tools (VPN, Tor, or Secure Proxies), or separate anonymizer software in order to increase privacy when you are using public Wi-FI.

Disable services through which you could be attacked. You should disable file sharing on your PC (it is preferred to block all incoming connections using your PC's firewall), services such as AirDrop on iPhone, etc.

Consider not using public Wi-fi. Consider not connecting devices containing the most valuable information to public Wi-Fi.

# 6 Digital identity

Use a separate set of identities (IDs and passwords) for your most valuable information and for your daily life. These IDs should not be connected with each other in any way (for example, one account should not be used for password reset of the other one).

Do not use the same password for all online services and web sites that you access. If you do that, and one of the services is compromised, intruders will get access to all other accounts of yours.

Use two-factor authentication for access of the online services whenever possible. Most of the popular services allow the use of two-factor authentication. This could be an application such as Google Authenticator, password sent over SMS, etc.

Attach on-line service to your device. Some services also allow attaching your device to your account. If you try to access the service from a new device, you will be prompted for additional authentication.

Use difficult-to-guess security questions to retrieve your password. Many online services offer you to set up responses to a set of common questions in order to gain access to your account in case you have lost your password.

These are typically standard questions, such as What was the model of your first car. You should realize that intruders could find out access to these questions by examining public property records, or the information that you post online in the social networks.

Ensure confidential information (and backups) are not stored in the cloud unencrypted. Beware that cloud service providers have full access to your information in the cloud. In case your data is encrypted, it can potentially be read by others, requested by authorities, etc. Use encryption tools, such as Boxcryptor www.boxcryptor.com/ru/ to encrypt the files that you store in Dropbox, Google Drive or iCloud.

Your digital footprint is a collection of information about you that consists of:

- Active footprint - everything that you post online yourself;
- passive footprint - information that web sites, on-line services and search engines collect about you;

You can google your first and last name to be surprised how much information is available about you on the Internet.
Your digital footprint defines your online reputation that can be used during background checks by potential employers, your counterparties or clients, authorities issuing visa, or by anyone else who wants to collect information about you, including potential intruders and spies.

Always think twice before posting anything online. Would this post contribute to your positive image? Does this give too much information about you? Does it allow someone to more easily attack you, or find out your habits in order to secretly search your apartment, or kidnap your children?

Consider disabling location tags in the photographs. Some services, such as Instagram, allow viewing time and location of the photos that you post online. These features can be used by others to find out a lot of information about you. On the other hand, if you are filming while attending protests, you may want to enable location tag in order to document what you evidence, and possibly use it in court.

Delete and disable your history on online services if you don't use them. Beware of your activity and search history in search engines, YouTube, online maps, etc. All this information is stored by the service providers, and may be potentially shared with the third parties (or leaked outside due to a security holw). Remove this information, and disable activity history unless you are using it.

Log off from your accounts if you don’t use them (rather than just closing a web browser). This decreases the risk of someone else using your account impersonating you.
Consider whether to use a real name, photo and email address when creating an online account.

Understand privacy policy and exact features of the online service. In particular, carefully study the privacy features of Google groups, understand differences between open, closed and secret groups, and what happens when the group is archived, it's administrator is blocked, etc. More information about it can be found here:
www.ssd.eff.org/en/module/facebook-groups-reducing-risks

Additional tips for protection on social networks:
www.ssd.eff.org/en/module/protecting-yourself-social-networks

## 6. 1 Google account

Run reports to check security and privacy settings of your Google account.
Consider pausing or disabling the following features, unless you use them. Use of these features may be considered very convenient, so it is a tradeoff between convenience and privacy:

Web & App Activity. Enabling this setting saves your activity on google sites, including history of web browsing, searches and your location;
Location history in Google Maps. Saves history of your daily movements and places that you visit;
Device information. Stores all data (contacts, photos, etc.) from your device in your Google account;
Voice & Audio activity. Enables you to issue voice commands to your phone, and stores those commands as well;
YouTube search and watch history. Saves history of the things you view and search for in YouTube;

Limit or disable use of location services. You can limit use of location services to a specific application, or disable it completely.
Limit Ad tracking in order to stop sharing your data with third parties.

Set access controls for your applications. You can granularly control whether you allow each application to access your microphone, calendar, photographs, etc.
Enable private browsing mode of your web browser (in case you use out-of-the box web browser).

# 7 Personal finance

Use a separate card for internet payments. If you want to pay online, it is recommended to have your bank issue a separate card for you for such purposes. You should transfer to this card only a limited amount of money that you need to make payments online.

Use limits offered by your bank. Set daily limits by amount and number of transaction, currencies and countries (this possibility is typically offered by your bank).

Setup OTP-approval. Most banks now offer OTP - One Time Password, required to authorise your transactions. For example, this could be an SMS password that your bank sends to you each time when online payment is initiated. You must enter a password provided to you by SMS into the online payment application in order to complete the payment.

Set up SMS-notifications for all movements on your account. Ask your bank to configure SMS-notification for every banking transaction. This would allow you to identify a fraudulent activity on your account.

Do not store your internet-banking digital key on your PC. In case your bank provides you with a digital key for encrypting and digitally signing your transactions, it is recommended not to keep this key on your PC. If your computer is compromised by hackers, your key will be stolen too, and used to make payments on your behalf. It is recommended to store the key on an external device, which is disconnected from your PC most of the time.

Don't use credit cards to pay online if you want anonymity. You can be tracked and traced if you use credit cards to pay. Consider using a prepaid card, or a cryptocurrency if you want an increased level of anonymity. Consider reading a separate guide on using bitcoins for anonymous payments: www.techradar.com/how-to/how-to-make-anonymous-payments-with-bitcoin.

## 8 Strong passwords

Instead of using passwords, use passphrases - sentences that consist of a number of words. These could be easy to remember for you, yet they will be much more secure than regular passwords. For example: My favourite Shakespeare character is Romeo!
The longer is your password, the more difficult it is to guess. Try to make the password be as long as possible.
Use special characters, and numbers. If you are restricted in the length of your password - try to use a combination of upper, lower case characters, letters and special characters. Do not use words (or names of your pets, cards, relatives etc.) - these will be easily guessed by special password hacking programs.

Use password managers to securely store and manage your passwords. There are a number of solutions out there, both free and commercial ones that can simplify management of passwords. Some of these tools can synchronize your passwords between your PC, mobile phone and tablet.

Use third-party comparison of password managers, and choose a tool that suits you:

www.pcmag.com/article2/0,2817,2407168,00.asp

Below is a step-by-step guide on the use of one of the cross-platform password managers: www.ssd.eff.org/en/module/how-use-keepassxc

Password manager can be hacked too. Beware that a password manager, like any program, could potentially contain a backdoor. Password manager, therefore, could be a good solution to simplify your everyday life. However, if you have your most sensitive data, creating a long password and storing it in a safe location is a better idea.

## 9 Home and close ones

Make sure your Internet router and Wi-Fi are set up securely. Change default settings and passwords on your devices. Use strong passwords. Make sure that you have NAT and a firewall setup to protect your home network from the Internet. Enable 802.11 security, hide your network ID, use MAC ID filtering if possible.

More and more home devices of yours can be accessed and controlled from the Internet. The list of devices includes security alarms, locks, air conditioning and lighting, refrigerators, etc. Some devices may contain cameras. Make sure that you at least change the default passwords on the device. Read carefully the owner's manual to enable built-in security features if any. Protect these devices with your home router firewall.

Your children and other close ones can be approached by strangers through the Internet (for example, via messengers, social networks or phone call), threatened or fooled into providing information. The messages they receive could sound very realistic, for example, assuring them that you need to send someone money in order to get you out of trouble.

Talk with your children and relatives and explain to them that they should not always trust information that they receive from strangers over the Internet. If they receive a call or a message from you, they should try to call you first in order to verify that the message is indeed from you.

If your account or device has been compromised you should completely reinstall PC or mobile device that has been compromised. You should also login from a clean device to all your online accounts and change your passwords and digital keys.

# ABOUT CONTRIBUTORS

**Adéla Klečková** (editor) works as a project manager for Friedrich Naumann Foundation for Freedom. She studied International Relations, European studies und Journalism at the Masaryk University in Brno. She gained experience from the fields of politics and diplomacy as an intern at German Parliament and Czech embassy in Vienna. Previously she worked as a foreign desk reporter at the Czech newspaper Economic Daily.

**Péter Krekó** is a social psychologist and political scientist. He is the executive director of Political Capital since 2011. He worked as a Fulbright Visiting Professor in the USA at the Central Eurasian Studies Department of Indiana University. He focuses on Russian 'soft power' policies and political populism and extremism in Europe. He is the member of the presidential board of the Hungarian Political Science Association. He was the co-chair of the PREVENT working group at the EU Radicalisation Awareness Network, and is currently an expert member of the EU RAN Centre of Excellence.

**Alice Stollmeyer** is a Digital Advocacy Strategist. She has lived and worked in Paris, Amsterdam and Brussels, the heart of the European Union. With a solid background in social science, science studies and communication, in 2012 Alice founded her own consultancy @StollmeyerEU, which specialises in EU public affairs, political communications and digital advocacy. She has been ranked a top digital EU influencer ever since. In 2016 @StollmeyerEU broadened its portfolio: previously focused on energy and climate policies, now its focus is politics, digital developments and European values like democracy, human rights and rule of law.

**Veronika Víchová** is an Analyst and a Coordinator of the Kremlin Watch Program at the European Values Think Tank. She graduated the Masaryk University in Brno. She co-authored a study on how Kremlin propaganda portrays European leaders which was published by The Atlantic Council and an Overview of countermeasures by the EU28 to the Kremlin´s influence operations. She compiles the Kremlin Watch Briefing, a weekly newsletter on disinformation and influence operations for more than 7.000 European experts, journalists and officials. She participated in the Transatlantic Fellowship Program in Washington DC organized by the World Affairs Journal, which she spent at the office of Senator Rob Portman.

**Alexey Yankowski** is an IT Strategy and Cybersecurity consultant with over 20 years of international experience. Having worked for PwC and Ernst & Young audit and consulting houses, as well as ING, Barclays and SAIC, Alexey had been exposed to a variety of clients across different industries. Alexey is also as a leader of the Kyiv Chapter of International Professional Association ISACA, whose mission is development, provision and promotion of research, standards, competencies and practices for the effective governance, control and assurance of information, systems and technol.

Péter Krekó Alice Stollmeyer Veronika Víchová Alexey Yankowski

# COUNTERING DISINFORMATION and PROTECTING CYBERSPACE

Manual for Liberal Stakeholders

Guidelines for the liberal politicians and opinion makers containing practical recommendations on how to fight disinformation and disinformation media. In the three chapters, following information can be found:

## Part 1: Hybrid Warfare 101: strategies, actors and figures

Introducing the new art of warfare. How to win a war without firing one single bullet? What strategies to employ in order to defeat your enemy with his own weapons: freedom of speech, liberal democracy and respect for human rights? How to meddle with the minds of the citizens of your or foreign countries?

## Part 2: Fake News: countering disinformation and hostile propaganda

Explaining best practices how to increase media literacy. Aims to explain not only how differentiate reliable source of information from a propaganda website. Provides guidelines what kind of behavior and interaction to avoid on the social networks. Presents new trends and ways of spreading hostile propaganda.

## Part 3: Cyber Security: staying safe in the virtual space

The protection of the cyberspace is a global concern that does no longer apply to the personal computer only. It includes all devices that can be connected to the global internet. These devices impose many new challenges, both behavioral and technical. In the era where data is considered to become crucial tool of influence, people have to be aware that their privacy depends on their own behavior on the Internet.

elf

Friedrich Naumann STIFTUNG FÜR DIE FREIHEIT