ISBN 978-9934-564-15-4

CAMOUFLAGE FOR THE DIGITAL DOMAIN

A FORCE PROTECTION FRAMEWORK FOR ARMED FORCES

Published by the
NATO Strategic Communications
Centre of Excellence

Authors: Sebastian Bay, Michael Batrla, Henrik Twetman
Contributors: Jacob Willemo, Piret Pernik, Liina Lumiste
Project manager: Henrik Twetman
Copy-editing: Anna Reynolds
Design: Karlis Ulmanis

Riga, February 2020
NATO STRATCOM COE
11b Kalciema Iela
Riga LV1048, Latvia
www.stratcomcoe.org
Facebook/stratcomcoe
Twitter: @stratcomcoe

CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

This publication has been produced in close collaboration with the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE). The initial research was undertaken by Michael Batrla who contributed to the NATO CCDCOE as a visiting scholar. We would like to thank the NATO CCDCOE for supporting his work and for peer review by their staff. We highly appreciate their valuable comments and assistance throughout the writing and publication process.

Table of Contents

> Malicious use of digital information poses a threat to armed forces by potentially compromising the confidentiality of information concerning geolocation, capabilities, tactics, and the future intent of friendly forces, or enabling and supporting an adversary's influence activities.

Introduction

The digital environment is an increasingly important dimension of the contemporary battlespace. While we have been focusing our attention on cyber-threats and systemic resilience, less attention has been paid to challenges arising from the malicious use of openly available digital information regarding military organisations.

An adversary does not need significant resources or advanced cyber capabilities to pose a threat in the digital domain, when social media and digital technologies are easily accessible, providing information and infrastructure that can be exploited by anyone with access to a computer and an internet connection. For example, open-source methods can be used to geolocate military units, social media can be used to augment influence activities, and social data can be *scraped* for valuable intelligence.

In 2018 the NATO Strategic Communications Centre of Excellence (NATO StratCom CoE) designed an experiment to demonstrate how an adversary could collect significant amounts of personal data on soldiers via open sources online, easily and at a very low cost, and how this data could be used to influence the behaviour of members of a target audience in tactical or operational contexts.[1]

The methods and infrastructure used to target individual soldiers can also be used on a strategic level to undermine decision-making processes within NATO or individual Alliance member states, or to attack public support for military operations.

While our understanding of potential vulnerabilities in the digital space is still developing, it is clear from a force protection perspective that we must improve our understanding and capability to safeguard personnel, resources, facilities, and critical information in the digital domain.

This report has been produced by the NATO StratCom CoE with support and assistance from the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) as a point of departure for discussion on force protection in the digital domain. It builds on the challenges and issues we have observed from working closely with various armed forces and military organisations, and is intended to support commanders and decision-makers in coming to terms with these issues. Our hope is not to provide definite answers, but to stimulate debate among Allies and Partners to find a productive way forward.

We first define the problem from a force protection perspective, describing the various ways in which digital technologies might be leveraged by malign actors to affect military operations. Then we provide an overview of emerging trends and risks in the digital domain. Finally, based on the identified challenges, we suggest a framework for countering the malicious use of digital information through assessing, preventing, and defending against such threats.

Understanding the problem

Evidence continues to accumulate that both states and non-state actors are increasingly able to access, collect, process, and disseminate digital information that can be used to:

- geolocate military units
- reveal capabilities and future intents of military units
- facilitate influence activities.

Open-source information has enabled terrorist organisations to identify active US military personnel,[2] citizen journalists to identify and track Russian armed forces in Ukraine,[3] researchers to reveal secret military bases,[4] and journalists to identify individuals working for secret government agencies.[5]

A range of experiments has also shown that the Alliance and its member states suffer from significant vulnerabilities in the digital domain:

- The NATO StratCom CoE successfully identified, targeted, and influenced soldiers participating in a military exercise in 2018.[6]
- Students at Tallinn Technical University were able to identify and locate Allied ships and sailors participating in a military exercise in 2018.[7]
- In 2016, a military exercise red-team[8] was able to engage the public to identify and geolocate military units within a timeframe that would have enabled kinetic targeting.[9]

NATO FORCE PROTECTION. *The survivability of any NATO-led joint force is a principal consideration in strategic planning and decision-making—with implications that extend well beyond the military mission and into issues such as public support and political cohesion. The Alliance and its forces remain vulnerable to a wide variety of hazards and threats […]. A threat may be described as having the perception of being in some degree of danger based on an overall assessment of the situation, taking into account own and adversary's capabilities, previous adversary actions, hostile intentions, etc. External threats and insider threats may also exist in environments considered to be safe, such as a home station or base or a forward operating base. Adversaries can be expected to exploit perceived Allied weaknesses and vulnerabilities, giving rise to the need for a comprehensive and resilient strategy for the protection of forces. Therefore, all military units must be able to defend and protect themselves appropriately against prevailing threats and hazards across a range of military activities throughout predominant campaign themes.*
–Allied Joint Doctrine for Force Protection 3.14[10]

The ability to identify and assess potential threats, risks, and vulnerabilities related to force protection in the digital domain is already critical for mission success and will continue to be so in the foreseeable future.

We intend this publication to support commanders and decision-makers in identifying and understanding threats and the threat environment, so they are better able to allocate the resources necessary for the protection of critical assets.

While risk elimination is not possible in most conflicts and scenarios, informed risk management can greatly improve a commander's ability to keep critical assets safe.

Trends and developments in the malicious use of digital information

Recent trends and developments in the malicious use of digital information could have significant consequences for armed forces:

- **Abundance**: In times of crisis or conflict, people tend to share information and documents, and to call for help or communicate with authorities through social media. Media and social media coverage of recent conflicts has resulted in far more hours of footage of a conflict than the actual duration of the conflict. This abundance of openly available information provides unprecedented opportunities for adversaries in relation to data collection and analysis.[11]

- **Accessibility**: Technological tools and guidelines for using them are easily available to anyone through the internet, including online black markets.[12] Digital expertise in collecting and analysing online information is no longer solely the purview of private-sector companies specialising in market analysis and intelligence services.[13] The same technical tools and online information are being widely used by malicious state and non-state actors to undermine democratic institutions globally.

- **Privacy:** Following a number of high-profile privacy scandals,[14] there is currently a shift towards more private and encrypted communication channels. Such channels provide users with more security; however, they also make detection and countering of malicious use more difficult. Furthermore, malicious actors have become more effective at covering their tracks.[15]

- **Manipulation:** Tools and techniques for impersonation, manipulation, and social engineering are improving. Technological advances such as 'deep fakes' (digital forgeries)[16] make it increasingly difficult to trust sources. Paired with limitations on social media platforms to control the automatic collection and processing of data, active methods (such as 'sock-puppet' accounts where real users control multiple deceptive accounts) are likely to become more important for digital information collection for both benevolent and malicious actors.

- **Aggregation:** Despite somewhat

> If everything is becoming a computer, then everything is becoming a potential surveillance device

improved privacy and security measures for users, social media companies and others continue to generate, collect, and analyse data about individuals to create custom online experiences, most commonly for marketing purposes. This raises concerns about how such data is processed and who benefits from it, as well as the risks associated with a lack of data security. Adversaries can access a wealth of personal data legitimately through commercial providers, as well as through cyber-attacks and involuntary violations of data confidentiality.[17]

- **Connectivity:** The Internet-of-Things (IoT) will continue its victory march across all human activities. Interconnected devices, such as fitness watches, smart home appliances, and network-connected medical equipment, can also serve as sensors, relaying potentially sensitive information about a person's habits and activities, health and vulnerabilities, social network and political affiliations that can be used to manipulate. As Bruce Schneider said, *'If everything is becoming a computer, then everything is becoming a potential surveillance device.'*[18] To add to the problem, such devices are often flawed from a security perspective due to systematic challenges inherent in such a high pace of development/deprecation for new technologies.

- **Speed:** The threat-and-vulnerability-landscape for digital information is highly dynamic and constantly evolving. The half-life of information technologies is decreasing, meaning that constant attention and adaptive solutions are required to tackle current and future challenges.

Risks in the digital space

Malicious use of digital information poses a threat to armed forces by potentially compromising the confidentiality of information concerning geolocation, capabilities, tactics, and the future intent of friendly forces, or enabling and supporting an adversary's influence activities. In this chapter we outline how such information can be obtained, analysed, and used by an adversary. We also provide several case studies to better illustrate why an adversary's malicious use of friendly information is a challenge for armed forces.

Discoverability of geolocation

Protecting the geolocation of personnel, equipment, infrastructure, and installations of military units is crucial for mission success. Today's digitalised society generates an abundance of open information that an adversary can exploit to obtain sensitive geolocation information. While geolocation information is easily accessed using digital sources, it can also be provided directly by conflict participants and the general public via digital platforms.

Geolocation data allows an adversary to discover and adapt to the position and movements of forces, thus serving as a tactical, operational, or strategic force multiplier. It also often enables or improves kinetic targeting and battle damage assessments. Geolocation data can also be useful information for enemy influence activities against friendly forces.

There are multiple means of obtaining geolocation information in the digital space:

- **Social media postings**

Most social media platforms provide an option (sometimes active by default) to geotag posts, enabling collection of social media posts based on a particular location, either directly or through commercial services. Some platforms (for example Snapchat) provide the geolocation of public posts on a map layout (in this case—Snapmap). This allows users to view posts based on geolocation. A number of commercial services, such as Echosec and Geofeedia, also offer advanced geolocation-based searches with geo-fences, image recognition, and alerts that enable advanced geolocation-based monitoring.

Geolocation can also be inferred from social media posts based on visual elements in pictures or videos. This technique is widely used by open-source intelligence operators and digital journalists for geolocating and verifying reports from conflicts—often quickly and with great accuracy.

CASE STUDY—Ukraine Conflict: MH-17, the Annexation of Crimea, Social Media, and Crowdsourced Information

The Bellingcat investigation of the downing of flight MH-17 in Eastern Ukraine is a prominent example of how social media can be used for geolocation purposes. This investigation was able to reveal location and identities of personnel and equipment in relation to the shooting.[19]

Hrabovo, Donetsk region / Ukraine - 07.25.2014
Crash site on July 17, 2014 of the Boeing-777 of Malaysia airlines, flight MH17 near Hrabovo village. Burnt wreckage on the plane in the field.

Bellingcat has used similar methods for other investigations, such as identifying Russian soldiers operating in Ukraine. Subsequently, the Russian State Duma passed a law to ban soldiers from carrying and using network-connected devices and sharing information related to their service.[20]

The Ukrainian conflict also saw other anonymous investigators and grassroots efforts, such as the hashtag #StopTerror (#СтопТеррор), through which crowdsourced information about Russian and separatist military movements in Eastern Ukraine were reported to Ukrainian authorities.[21]

Crowdsourcing information

Geolocation information about military units can also be crowdsourced—a call for information can be posted to a network of social media users who collect, aggregate, and share information with each other. The power of this becomes especially apparent during conflicts or crises when individuals tend to collect and share information about military activity. This method of information sourcing is particularly popular with digital investigative journalists, non-governmental organisations (NGOs), and ordinary citizens focused on uncovering information about wrongdoing, such as (war) crimes, human rights abuse, or corruption. However, the information used for the purposes described above is available to anyone, including malicious actors.

MICROSTUDY—DARPA

In 2009 the Defense Advanced Research Projects Agency (DARPA) conducted an experiment to explore the roles the Internet and social networking play in solving broad-scope, time-critical problems. The experiment, set up as a challenge, was for teams to be the first to locate ten red weather balloons at ten random locations in the United States. A team from the Massachusetts Institute of Technology (MIT) won by locating all balloons using crowdsourcing in under nine hours.[22]

▪ Application-generated position data

App-generated position data and metadata are other possible sources of geolocation information generated by the various sensors embedded in virtually every modern handheld device. Geolocation data is often collected by third parties, such as data brokers, to be used for targeted advertisement. This tracking can even be cross-app, cross-device, and cross-domain (implying the possibility of cross-referencing digital profile data with data from activities that occur outside of digital platforms, such as credit card purchases). The privacy and security of such data is not always transparent or fully controllable by users. For example, a user's geolocation can be triangulated by purchasing targeting advertisements on social media that use app-generated position data.[23]

MICROSTUDY—Geolocation Data

In April 2019, the Swedish newspaper *Dagens Nyheter* investigated the availability of geolocation data from commercial vendors. The newspaper successfully identified and tracked individuals visiting or working at the Swedish Security Police, the Swedish Armed Forces, and the Swedish National Defence Radio Establishment by conducting geolocation searches in data sets bought from commercial data brokers. The individuals were identified by tracking the mobile phone geolocation during the day (when people took them to work) and during the night (when people took them home). Interviews with some of the individuals identified confirmed that they were unaware their data was being collected and sold to third parties by various applications.[24]

IoT-generated data

IoT-generated data include a diverse body of sensors and devices that often record and contain geolocation data and metadata. Fitness devices and tracker apps that provide the option to publicly share geolocation data are among the most prominent examples. The use of such IoT devices is expected to rise in the future. Additionally, fitness devices are specifically aimed at younger people who follow the trend to frequently monitor their health and fitness. Unsurprisingly, this group is well represented in militaries as the following case study demonstrates:

CASE STUDY—The Internet of Things and Fitness Tracker Apps

The problem with military and intelligence personnel inadvertently leaking information through fitness apps emerged in 2018 when such information enabled researchers to determine the geolocation of sensitive military bases as well as the personal data of investigated subjects. While both fitness app companies and military organisations took steps to address this problem, it remains a challenge.

To check on the current status of this issue, the NATO StratCom CoE conducted a limited experiment on a fitness app service website. During this experiment, no interaction was conducted vis-à-vis investigated persons and no personal information was gathered, stored, or shared.

On one of the military bases studied, a particular fitness app was used to log twenty user-generated running and cycling tacks in April 2019, recording 'attempts' for each track. Participants engaged in more than 12,300 running 'attempts' and 3,500 cycling 'attempts'. The study excluded app-hosted tracks nearby but outside the base, (such as the 'Air Force Half and Full Marathon', which, despite the name, took place off base).

It should be noted that the number of attempts on the tracks does not reveal the actual number of personnel on the base, but it does provide a rough indication. It is also necessary to acknowledge that users may log on using an inauthentic online identity and/or a falsified GPS location (which can in itself be a security risk).

The following results were recorded:

- At the time of the experiment, the latest activity registered by the app was only a week old, indicating recent usage despite the military having social media policies in place to limit the spread of digital information.
- The majority of users had posted their full name and address to the app's leader boards, often also making a photograph publicly available.
- Users who publicly revealed only a general address (such as city/state) would often inadvertently reveal their home address, as it could be inferred from other completed segments or photos.
- Users' track records sometimes depicted travel outside the base (likely patrol duty or even operations).
- Photos and/or exercise details sometimes depicted family members and other close people (e.g. 'running with wife', 'exercise w/son', etc.) or other information that could be used to identify the unit and its other members.
- It was possible to infer information that could be used to identify military personal by using the 'followers' function or by reading comments to users' activities. Sometimes, the publicly available addresses of followers stated their military base.

For an adversary, such apps can provide valuable information, such as individual and unit identification, or troop rotation cycles that could be used to support an adversary's kinetic or non-kinetic targeting. Additionally, such publicly available information can often be used to gain access to other sources and methods of collection.

- **Satellite, aerial, and fixed livestream imagery**

The rapidly increasing availability of satellite imagery, e.g. through publicly available or commercial providers, enables monitoring of, for example, changes in infrastructure or military movement.

Similarly, the growing ubiquity of inexpensive and easily acquirable remote-control, programmable unmanned aerial vehicles (drones) enables various actors to monitor the locations and positions of military units.

An abundance of sources for fixed livestreaming video, such as road cameras, wildlife cameras, and weather cameras, provides remote monitoring of specific locations. Sometimes this type of sensor is part of a protected system that would need to be breached to gain access, but other times they are openly accessible online and can be found via search engines such as Shodan (a search engine for internet-connected devices).

MICROSTUDY—Non-State Aerial Reconnaissance Teams

During the conflict in Ukraine, Ukrainian civilians established so-called 'volunteer aerial reconnaissance teams' that used commercially available small unmanned aerial vehicles to produce aerial imagery of separatist and Russian forces, which was then allegedly sent to open-source research groups and to the Ukrainian authorities.[25]

Such systems have also been successfully used elsewhere, for example by terrorist organisations or drug cartels. DAESH used aerial reconnaissance in Syria for targeting, drone strikes, and —most prominently—for recording terror attacks in support of DAESH influence activities.[26]

- **Location information systems specific to sea- and air-based vehicles**[27]

Information systems such as Flightradar24 and Marine Traffic can be used to collect real-time information about air and sea traffic.

Even if a vessel isn't logged by one of these systems, crowdsourcing by plane- or ship-spotters[28] often adds unregistered traffic to air and sea traffic monitoring platforms. Information about air and sea traffic, such as registration numbers and route information, can also be collated with other types of information such as social media postings to identify passengers, sailors, and aircrews, which then makes it possible to geolocate their activities.

MICROSTUDY—Bellingcat Open Source Monitoring of the NATO Trident Juncture 2018 Exercise

In general, there is more open-source information available about military exercises than about actual military operations, which tend to be classified. Nonetheless, exercises can be used to showcase some of the procedures, methods, techniques, and sources that adversaries could leverage during a military operation. Bellingcat's coverage of NATO Trident Juncture 2018 serves this purpose.

Bellingcat obtained data from social media by following popular hashtags (#TridentJuncture, #NATO), and the social media accounts of relevant public figures and organisation press services. Valuable information was also obtained directly from military exercise participants and local inhabitants by the use of geotags in posts and pictures. Bellingcat notes that: *'Soldiers who take part in large-scale exercises, regardless of nationality, love to share photographs of their trip on social networks. (...) it is hard to stop a 19-year-old conscript or new contract soldier from sharing photographs on Instagram of themselves in interesting locations surrounded by impressive military hardware."*[29]

Bellingcat also showed how commercial satellite data and other services such as Marine Traffic, ADS-B Exchange, FlightAware, Vessel Finder, etc. provided able data about Trident Juncture.[30]

Discoverability of capabilities and intents

NATO defines capability as 'the ability to perform actions to achieve desired objectives/ effects'.[31] Digital information can be maliciously used by an adversary to collect intelligence regarding capacity and intent, and to degrade the capability of NATO forces. The sensitive information that can be obtained through open-source information includes details about military and government personnel, numbers and types of military equipment including vehicles and supplies, and information about the tactics, techniques, procedures, and training standards of troops.

The publicly available online information sources that can be used by adversaries to obtain information about friendly military capabilities are similar to those used for geolocalisation, but there are some differences.

Social media posting

Information about capabilities is generally obtained from a combination of social media information, directly from conflict participants, their families and acquaintances, and from the general public. For example, it is common to see social media posts from military personnel showing photographs of equipment, showcasing unit size and composition, and displaying tactical behaviours.

Similarly, it is common for spouses or partners of military personnel to upload content specifying when and where their loved ones are being deployed. It is also common for civilians who observe military activities to upload photos and videos to open platforms.

This type of information can be correlated with official sources, such as professional or semi-professional media and official military communications and visual media, to acquire useful open-source intelligence.

MICROSTUDY—MUMBAI 2008

A dated, but informative example of the malicious use of digital information is the 2008 Mumbai terrorist attacks, where the terrorist organisation Lashkar-e-Taiba coordinated 12 bombing and shooting attacks over four days, leading to the death of at least 174 people.[32]

During the preparation phase, terrorists used open-source data (e.g. Google Earth imagery) paired with live reconnaissance to assess targets and familiarise the attackers with the environment.[33]

During the terror attack a remote command-and-control post collected and analysed information from online news and social media to infer the positions and intentions of Indian responders. This command-and-control post relayed information through VoIP (Voice over Internet Protocol) technologies, cell phones, and satellite phones to provide their tactical teams with situational awareness, and for basic command and control.[34] This simple use of publicly available data proved to be an effective force multiplier for the terror group.

- **Online impersonation and social engineering**

Impersonation and social engineering attacks on soldiers or civilian populations play a major, and likely increasing, role in data collection.

Through techniques such as honey-trapping or scamming, individuals can be manipulated into unknowingly providing sensitive information to an adversary.

Social engineering attacks often use fear and extortion, flattery and seduction, or greed. These techniques have repeatedly been used for red-teaming in military exercises with significant success, indicating the scope of this vulnerability.

- **Crowdsourcing information**

Information about capacities and intent may be willingly or unwillingly passed to an adversary by crowds with ubiquitous mobile devices and by social media postings by individuals in physical proximity to a military operation. Hybrid/non-state actors participating in conflicts have set a precedent for using crowdsourcing techniques to identify and analyse military infrastructure, equipment, and procedures.

MICROSTUDY—The 2019 Hong Kong Protests: Crowdsourced Intelligence and Encrypted Apps

Fearing digital surveillance by Chinese authorities, the Hong Kong anti-extradition law protesters utilised end-to-end encrypted Telegram chats (with up to 70 000 members) to report on police force locations, capabilities, and intents. They also used an integrated voting system to decide on the next course of action or on the locations of future demonstrations.

China allegedly tried to limit their activities by DDoS (Distributed Denial-of-Service) attacks on Telegram servers, but had limited success.[35] Moreover, if access to one service was hampered protesters could simply migrate to another one, such as Wire, Riot, or Firechat, services that were used during similar protests in 2014. These services support an option for creating mesh networks through Bluetooth, Wi-Fi, or peer-to-peer WiFi, effectively circumventing congestion on cellular networks and avoiding the possibility of losing service because of server shutdowns.[36]

- **IoT-generated data**

Information about military capabilities, such as personnel and equipment numbers, can be obtained from civilian and commercial sensors, such as footage from publicly available or misconfigured traffic and CCTV cameras.

- **Satellite and aerial imagery**

Even adversaries with few resources can benefit from publicly and commercially obtainable satellite imagery. However, as image resolution is often limited and flyover times are predetermined by operators, satellites will not always provide the necessary information, which is why the use of aerial reconnaissance is also prevalent, especially among non-state/hybrid actors and terrorist groups, provided by, for example, small, inexpensive, and easily acquired UAVs (unmanned aerial vehicles).

USS New York docked into Plymouth after completing exercise Trident Juncture.

CASE STUDY—NEPTUNE 2018 at Tallinn University of Technology

Neptune 2018 was a cyber-security challenge conducted by Tallinn University of Technology during the NATO SaberStrike and Baltops 2018 exercises. During the exercises, groups of students were tasked with collecting as much open-source data as possible regarding the geolocations and activities of ships from Standing NATO Mine Countermeasures Group One (SNMCMG1) participating in the NATO exercises.[37]

The information gathered was purely open source and included media and military press releases, sailors' social media activity (notably Snapchat, Facebook and Instagram), geolocations from IoT devices (notably fitness trackers), and publicly available port cameras found through Shodan.

The result of the students' open-source information gathering and analysis were impressive. Without any previous experience in open source information gathering, the students were able to discover and monitor ship positions with sixteen-second to five-minute delays.

The intensive location coverage was mostly enabled by improper settings of Warship-Automated Identification Systems (W-AIS), such as Maritime Vessel tracker, which were 'leaking' ship identification to tracking websites. W-AIS systems should be set to the 'NATO Warship' setting, but in this case (and numerous others as can be seen on tracking websites) they were set to show information that often included full or partial ship names and designations. These identification systems served as a springboard for further collection of geolocated data from social networks, which meant that even ships with proper W-AIS settings were being identified.

Other information obtained included activities and objectives, locations, plotted courses, and future port destinations, as well as weapons capacities and ranges, and details about onboard staff. Public data on personnel included user account credentials for various national and NATO military email addresses obtained from 'leaky' external (public) websites.[38]

CASE STUDY—Open Source Research Groups and the Ukraine Conflict: InformNapalm

During the conflict in Ukraine a new type of crowdsource investigation group emerged. The volunteer group InformNapalm stands out from other crowdsourcing groups because it actively collected information on the ongoing conflict as a party to the conflict.[39]

InformNapalm aimed to uncover and publicise information regarding Russian activities in Eastern Ukraine and alleged violations of the Minsk ceasefire agreements by separatist forces.

While materials from social networks and satellite images served as the basis for their investigations, they differed from other investigative groups by also actively collecting data.

Among other techniques InformNapalm used:

- Researchers and volunteers in the conflict areas. These included volunteer aerial reconnaissance teams who produce aerial imagery using commercially available drones.
- Cyber activities. The group partnered with Ukrainian hacker groups and published leaks pilfered from Russian and separatist officials (e.g. the Surkov Leaks).[40]

InformNapalm focused on finding and mapping checkpoints, infrastructure, personnel, and equipment; analysing terrain and possible enemy actions; monitoring channels of communication; and publishing personal information about Russian soldiers.[41]

InformNapalm tried to take an active part in the conflict themselves by exerting influence on the Russian government through issuing ultimatums as an "asymmetric response [to] the "hybrid" actions of the Kremlin in both Ukraine and Syria".[42] To this end InformNapalm repeatedly doxed and shamed Russian soldiers, including adding the names of more than 2400 military personnel to a 'Russian Aggression Database', and published a list of 116 crew members of the alleged Russian Air Group in Syria.

Influence activities

'Defeat of an adversary, by whatever mechanism, is a cognitive outcome. (...) The accumulated stresses of combat and combatants' perceptions of a situation leads to fear, flight, or surrender. Alternatively, a force's commander perceives the opponent's relative advantages as a battle unfolds and concludes (through cognition) that the cost of continuing will exceed the possible benefits.'
- Paul, et.al, 2018.[43]

In a military context, influence activities are mainly used for three purposes:[44]

- for preserving and protecting freedom of manoeuvre in the information environment,
- for influencing behaviours, perceptions, and attitudes of target audiences and,
- for countering an adversary's propaganda and targeting their command and control functions and capabilities that support opinion-forming and decision-making processes.

All influence activities depend on accurate and timely intelligence in support of target audience analysis. The more you know about your audience, the easier the audience is to influence. The contemporary digital space with its abundance of openly available data provides unparalleled opportunities to target influence activities with precision. It is easy to see how detailed personal information aggregated from social media, data brokers, and other open sources can be used to harass, extort, or blackmail individuals, or to execute very accurate micro-targeting of strategic communication efforts and psychological operations.

Digital infrastructure also provides the platforms on which these activities take place. Techniques such as impersonation and social engineering are already being used in connection with military exercises and conflicts to influence behaviour of military personnel. On a strategic level, disinformation and broader propaganda efforts impacting, for example, mission support or public opinion occur in a similar fashion.

Accurate and timely intelligence is necessary for both influence activities and wider intelligence collection. Influence activities can, however, also be used to support intelligence gathering. There are multiple recent examples where military personnel have been influenced to provide information about their current whereabouts, gear, ammunition, mission, and intention by operatives using fraudulent social media accounts. Using influence activities in support of intelligence collection has become more common in the last few years.

The risk of malicious use of digital information is likely to increase, as advances

in AI technologies will continue to advance opportunities for malicious influence activities, for example, through the use of 'deep-fakes' (digital forgeries) or predictive modelling.

CASE STUDY—NATO StratCom CoE Red Team Experiment

The NATO StratCom COE conducted an experiment to assess if it would be possible to collect information on a military exercise, and if that information could then be used to successfully influence the behaviour of soldiers participating in that exercise.[45]

A research team was embedded within a red-team cell to evaluate how much data they could collect about exercise participants. They tested various open-source intelligence techniques to acquire data and tried out a range of influence activities to determine if it was possible to induce certain behaviours in the soldiers, for example, leaving their positions or not fulfilling their duties.[46]

The researchers used methods such as social media monitoring, targeted advertisement, impersonation, honeypot pages on social media, social engineering, and scraping of open-source databases. Most of these methods were employed over the main social media platforms—Facebook, Instagram, and Twitter.

With few personnel, less than a month of preparation, and an advertisement budget of approximately USD 60, the team was able to collect detailed personal information including names, phone numbers, e-mail addresses, pictures of equipment, names of family members and partners, and dating app profiles. The team managed to identify more than 150 individual soldiers, pinpoint the exact location of multiple battalions taking part in the exercise, gain knowledge of troop movements (including high-value units critical for mission success), and discover the dates of the active phases of the exercise.

This information was successfully used to craft targeted influence activities that induced behaviour undesirable to the target exercise, such as individual soldiers leaving their positions against orders.

The experiment showed that, at the current level of information security, an adversary is able to collect a significant amount of personal data on soldiers participating in a military exercise, and that these data can be used to target messages with precision, successfully influencing members of a target audience to carry out behaviours desired by an adversary.

Implications

There is no doubt that state, non-state, and hybrid actors will continue their malicious use of digital information and digital infrastructure in support of both kinetic and non-kinetic operations in near-horizon conflicts. The main channels will likely remain social media and mobile devices, due to their versatility and ubiquity—features that greatly enhance their appeal for intelligence collection, military operations, covert actions, and clandestine signalling. Adversaries turning these capabilities into effective weapons in the digital domain present a major challenge to NATO,[47] its Allies, and Partner nations today and in the future.

Malicious use of digital information will likely be even more common in the future for two reasons:

- First, less-resourced actors can use digital information for planning and execution, as this is much less costly than other collection efforts, such as signal intelligence collection, cyber espionage, or using human informants.

- Second, the amount of data to exploit will continue to increase. As IoT technologies gain prominence, there will be an even greater push for the collection and utilisation of personal data acquired through various sensors. Contemporary digital advertising systems combined with product design that is often lacking sufficient privacy or security mechanisms are likely to enable malicious actors to harvest these data by legal and illegal means.

Based on available research, case studies of the contemporary digital environment, and our experiences from working with various armed forces and military organisations, we draw the following conclusions:

Digital technologies are changing the operational environment

Allied armed forces are likely to operate in an environment in which (malicious) actors can effectively, and often in almost real time, monitor Allied movements and capabilities, and infer plans and objectives through malicious use of digital information. The risk will vary depending on the operational environment and its interconnectedness—there is greater risk in more populated areas.

Malicious use of the digital information is likely to enable adversaries to leverage asymmetric effects more effectively in the future. This includes reconnaissance, surveillance, and command-and-control support for kinetic operations, and non-kinetic

measures such as enabling and enhancing influence operations.

These findings are supported by our own experiments as well as by recent forward-looking research;[48] they also follow a recognised pattern where actors leverage common technology in unconventional ways to offset the technology advantage of an adversary.[49]

States should also expect further dilution and 'democratisation' of capabilities, technologies, and knowledge previously reserved for them. Combined with an often flexible and decentralised structure for the acquisition and sharing of intelligence—both vertically and horizontally. There is a risk of malicious actors becoming more effective and flexible using open and crowdsourced information, potentially surpassing the speed of more bureaucratic decision-making and command-and-control loops.

Adversaries are developing their digital toolbox

Adversaries are becoming more skilled at reducing the effectiveness of Allies' digital collection efforts. This is accomplished using a range of actions, such as:

i. more effective procedures for controlling digital signatures[50]

ii. enhanced ability to generate open-source false positives, which might include the conduct of military operations for the sole purpose of obtaining photos and videos for later use[51]

iii. increased use of privacy-enhancing tools and encrypted communication[52]

iv. increased ability to counter remote imagery collection efforts.

Naturally, the list is non-exhaustive and likely to change in response to specific interactions between available measures and countermeasures. Given how malicious actors use and share organisational learning,[53] often obtained through their own experience of the consequences of inadequate operational security (OPSEC), increased competitive ability in the digital arena is likely to be a goal for most future state, hybrid, and non-state adversaries.

If potential opposing forces have relatively high levels of technical expertise, malicious use of digital information is likely to impact Allied countries far more in future conflicts. Future opposing forces may establish measures for information control that are not available to Allied countries for legal or ethical reasons.[54] Conversely, malicious actors may sometimes orchestrate increased news and social media coverage in order to obtain more open-source information, so that they may better monitor enemy movements and plans, thus allowing them to offset some force and/or intelligence advantage.

Here it is also important to note that exposing

Russia as responsible for the downing of the MH-17 airline in 2014 does not seem to have changed Russian behaviour, with the exception of new restrictions on soldiers' cell phone use in combat zones. The exposure has had no discernible effect on Russia's wider ambitions or operational course in Ukraine, because the Kremlin is able to conduct influence activities to quell internal dissent and neutralise negative stories.[55]

Digital information will augment influence operations

High-ranking military personnel, decision-makers, and their families should expect to be targeted by highly personalised influence campaigns. Such campaigns might include a range of activities from doxing[56] of sensitive information, smear campaigns, and impersonation to direct intimidation, blackmail, and subversion. Disinformation will be a central component of any such activities.

Allied militaries are likely to be more vulnerable to the malicious use of digital information than potential adversaries. While our adversaries have been exposed to various levels of intelligence collection, and are becoming more practiced at taking countermeasures of their own, the leading generation of soldiers and officers in the Alliance have not previously had to question their reliance on digital technologies and on the electromagnetic spectrum, and the devastating effect compromised information can have on military operations has not been experienced for decades.[57]

These increasing risks and vulnerabilities mean that a practical guide created from a force protection perspective is needed as the armed forces develop their ability to counter the malicious use of digital information. The following chapters present a framework for understanding the challenges we face and mitigating the inherent risks.

Framework for countering malicious use of digital information

The framework laid out in this report is intended to support commanders' understanding of the problem as they consider the malicious use of digital information as part of the overall force protection process.

The *Allied Joint Doctrine for Force Protection* (AJP 3.14) provides an in-depth description of NATO's force protection process, which consists of a set of sequential functions built around an assessment of threats/hazards, vulnerabilities, and risks.

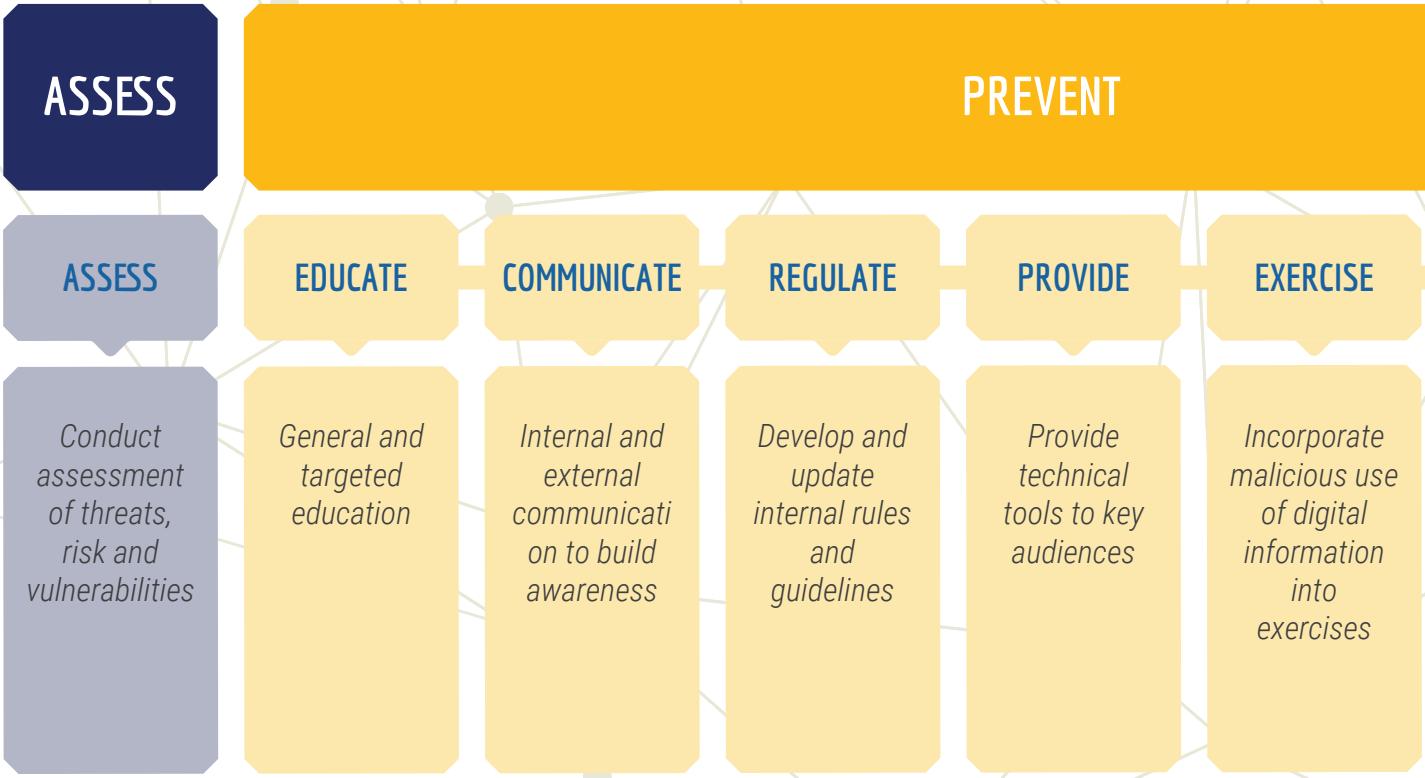
The idea for this framework was born out of the experience of conducting a large red-team experiment in 2018. To develop a framework for countering malicious use of digital information a number of workshops were held with subject matter experts throughout 2018. The outcomes of the workshops were further refined through literature reviews and in-house analysis and assessment. The final framework is based on some of the core principles of AJP 3.14, and it is intended to support conceptualisation of the problem.

This framework **should not** be seen as a step-by-step procedure. Most actions armed forces need to take are continuous and often must be performed in parallel with others.

This framework **should** be seen as a general checklist that identifies areas commanders need to consider in order to ensure force protection against the malicious use of digital information.

The framework for countering malicious use of digital information is divided into three parts:

- **Assess**: A thorough baseline analysis is the first step for any contingency planning. Any organisation must assess the risks and vulnerabilities associated with the malicious use of digital information as a prerequisite for further activities.
- **Prevent**: Pre-emptive measures should be implemented to strengthen an organisation's capacity to identify and manage the malicious use of digital information, and to deter or disrupt an adversary.
- **Defend:** Defensive actions, such as focused efforts to identify and counter digital disinformation, must be taken in order to protect from the organisation from attack in the digital domain.



Assess

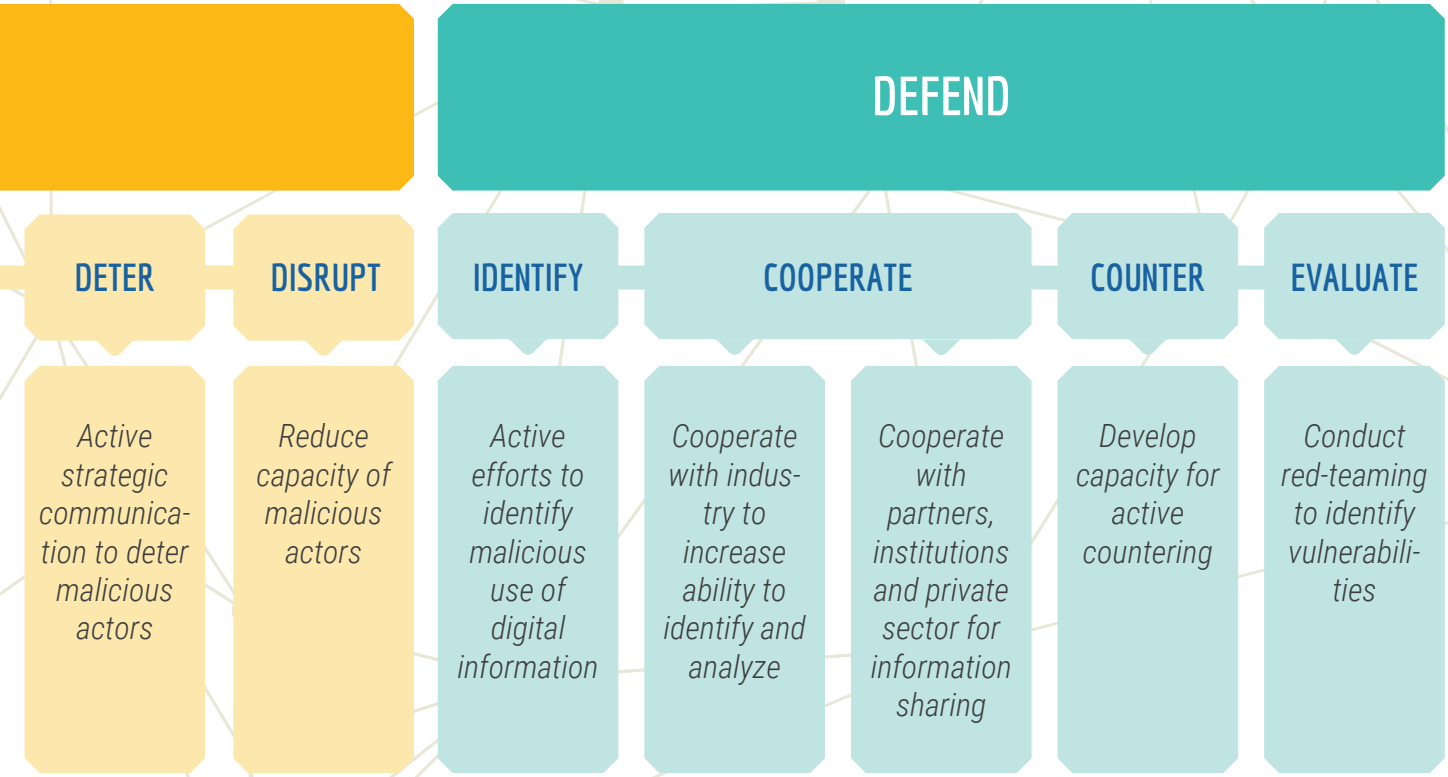
Conducting a thorough assessment is a critical first step for mitigating risks in the digital space. While assessment should naturally precede activities, it is important that assessment occur continually and in parallel with other measures, to ensure up-to-date situational awareness.

Conduct threat, risk and vulnerability assessments

Military commanders, agency officials, and operational planners should make formal risk assessments using a formula that considers the value of assets, the nature of existing threats, known vulnerabilities, and the potential impact of any loss of critical information to an adversary.

Vulnerabilities in this field exists wherever an adversary can collect or leverage digital information in a way that is detrimental to the mission. Therefore, identifying critical digital information, and assessing the associated threats, risks, and vulnerabilities, will be critical for mission success.

Although commander-level analysis cannot sufficiently substitute for responsibility and



vigilance at the level the individual soldier or sailor, careful consideration regarding targeted measures for OPSEC before, during, and after any operation will continue to be very important.

Questions for the threat, risk and vulnerability assessment

When conducting a threat, risk, and vulnerability assessment for countering malicious use of digital information, the responsible parties musk ask what vulnerabilities may exist that could allow adversaries to gain access to sensitive digital information that they could use for malicious purposes. We have listed a number of sample questions to inspire a discussion regarding questions relevant to the specific unit, mission, and area of operation.

- **Physical and digital infrastructure in AO**
  - How interconnected is the Area of Operation (AO)?
    - What types of sensors/IoT devices (e.g. traffic/CCTV cameras, automated road or forest management systems, etc.) are in the AO? Is it possible to use them to monitor allied forces in the AO?

    - Who exercises control over these sensors?
    - Are the sensors openly accessible, either through publicly available services (incl. IoT 'search engines', such as Shodan), or through misconfiguration or other easily exploitable vulnerabilities (e.g. unpatched software, default passwords, etc.)?
  - How will we monitor for new fixed sensors in the AO?

- **Human terrain in AO**
  - How technologically and digitally capable is the local population?
    - How likely is it that the local population will collect and distribute critical information?
    - Are local nationals connected to broader crowdsourcing and adversary networks?
    - Will the adversary be able to use local nationals for crowdsourcing?
  - Should allied forces expect external actors (state or non-state) to intervene through malicious use of digital information on behalf of the adversary?
    - How and with what capabilities?
  - Are allied forces able to monitor the local information environment to determine whether critical information is being shared online?
  - What are the conditions and vulnerabilities that adversary forces would be able to exploit when conducting influence activities aimed at the local population?

- **Allied forces vulnerabilities (home and in AO)**
  - Is it possible to effectively restrict the use of allied armed forces' personal devices (mobile, IoT)?
    - Are soldiers themselves likely to leak critical information (textual, visual, or audio) intentionally or due to misconfiguration?
    - Are soldiers' families themselves likely to leak critical information (textual, visual, or audio) intentionally or due to misconfiguration?
  - Are allied forces able to monitor the information environment to detect leaks of critical information in a timely manner?
  - Are adversary forces able to collect information about allied armed forces personnel that could be leveraged for influence activities?
  - Are allied forces able to identify and counter hostile influence activities aimed at Allied forces?
  - What are the conditions and vulnerabilities that adversary forces would be able to exploit when conducting influence activities aimed at Allied forces?

Prevent

Pre-emptive measures that create systemic resilience against the malicious use of digital information are a vital safeguard, denying the adversary opportunities to act. Raising awareness about potential risks related to the

digital information environment is a critical first step, but this general awareness needs to be augmented with specific education activities, communication measures, evolving regulations, and other activities.

Educate

Education is effective in countering the malicious use of digital information.

Effective education should target both internal and external audiences regarding means and methods to protect Allied forces' operational security.

Principles for using social media and for digital behaviour in general need to be incorporated into basic military training and consistently exercised, similar to fire-safety and first-aid training. The training also needs to be regularly updated, using recent case studies[58] and developments.

Effective education also requires the continuous education of Allied forces personnel and their family members regarding risks and safe practices.

'As infrastructure and security systems improve (e.g. firewalls), the incentive for social engineering attacks changed. Today, the manipulation of social media is the most cost-effective way of acquiring sensitive information. We should not forget that it is often the weakest link in a system that is targeted—even if your own social media privacy settings are strong, malicious actors may still be able to gather information on your friends or family members.' – Bittner & Carrigan in Willemo 2017.[59]

RESOURCES FOR CYBERSECURITY AWARENESS TRAINING

NATO Cooperative Cyber Defence Centre of Excellence Cyber Awareness e-course: https://ccdcoe.org/training/cyber-defence-awareness-e-course/

U.S. Department of Defense Social Media Education and Training: https://dodcio.defense.gov/Social-Media/SMEandT/

United Kingdom Social media guide: https://www.gov.uk/government/publications/using-social-media-a-guide-for-military-personnel

Communicate

Use communication to build awareness.

Communication is a valuable tool for raising awareness of the risks associated with the digital domain on a broader level. It should be integral to any strategy for countering the malicious use of digital information and should include both internal and external audiences.

Communication is not just what you say. It is also what you do and how you act. Armed forces should adopt a posture that signals the importance of digital security, and act to continually confirm their commitment to force protection in the digital domain to both internal and external audiences.

Regulate

Develop and update internal rules and guidelines.

Armed forces should continuously develop internal rules and guidelines regarding the use of digital devices and services, including social media. Due to the dynamism of the digital environment, rules and guidelines need to be frequently re-evaluated to ensure their continued relevance.

Easy measures, such as removing soldiers' smartphones and other devices, limiting connectivity, or restricting social media use, are beneficial in specific situations. However, during longer operations or during peacetime different rules and guidelines are needed, as each situation requires its own unique solution.

Armed forces should develop standard operating procedures for using devices and services during and outside of military operations and should ensure that these procedures are effective and up to date.

Equip

Provide technical tools and support to key audiences.

In today's digital space, our personal and work identities are interwoven. This means that risk is not confined to state-of-the-art government/military networks and devices. Malicious actors commonly target the weakest link, such as untrained family members, and unprotected personal devices or accounts.

If an adversary successfully manipulates military personnel to install a compromised app on a personal device, it could be as damaging as breaching a protected military network; this could have a tangible impact on military operations.[60] Likewise, targeting soldiers through their relatives, either by cyber or influence means, can potentially reveal sensitive information important for mission success.

Based on private sector experience and best practices, Allied armed forces should be more proactive about securing the homes and families of armed forces personnel.

The issues discussed above must be further investigated to identify potential safeguards that militaries/governments

could implement to protect armed forces and related personnel, for example:

- Provision of software solutions such as antivirus suites or VPN subscriptions, and protected hardware such as home Wi-Fi routers, to enable personnel to increase their privacy and security.

- Provision of expert training and support to ensure safe private digital environments for key audiences, including social media management training.

Train

Incorporate digital risk training into military exercises.

Armed forces should incorporate scenarios regarding the malicious use of digital information into training exercises, to increase commanders' ability to maintain force protection in the digital domain.

Experience from red-teaming conducted during domestic military exercises has positively impacted awareness and readiness throughout military ranks and has served to remind commanders of the importance of the protection of digital information to operational security and strategic communication.

Skills, tools, and methods for countering the malicious use of digital information can be developed, tested, and honed under proper conditions.

Deter

Deploy strategic communication to deter malicious actors.

Active and effective strategic communication efforts should be conducted to deter malicious actors. For NATO, strategic communications is the coordinated and appropriate use of NATO communications activities and capabilities in support of Alliance policies, operations, and activities, and in order to advance NATO's aims. [61] Such activities include public diplomacy, public affairs, military public affairs, information operations and psychological operations.

NATO strategic communications aim to[62]:

i. Contribute positively and directly to achieving the successful implementation of NATO operations, missions, and activities by incorporating strategic communications planning into all operational and policy planning.

ii. Build awareness, understanding, and support for specific NATO policies, operations, and other activities in close and lasting coordination with NATO nations.

iii. Contribute to the general public awareness and understanding of NATO as part of a broader and on-going public diplomacy effort.

NATO strategic communications should also be targeted to reach specific objectives such as deterring malicious activity.

Disrupt

Reduce the capability of malicious actors.

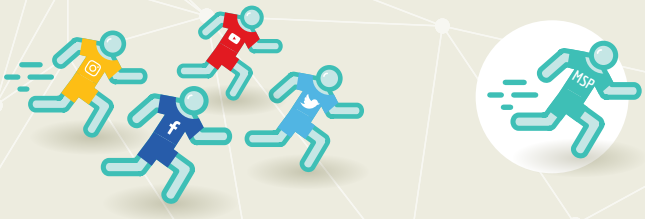
Allied forces should detect and disrupt the capability of opposing forces to maliciously use digital information and its supporting infrastructure.

On a strategic level such activities can range from detecting and disrupting botnets to reporting fake profiles, sites, bots, and 'cyborgs' used for influence activities to social media companies.

On an operational level, activities will include disrupting hostile crowdsourcing, blocking and/or removing hostile or vulnerable sensors, and disrupting the technical infrastructure used by opposing forces.

Allied forces also need to support friendly platforms (especially social media) to close technical loopholes and bugs that can endanger user data even when sufficient privacy measures are implemented.[63]

FALLING BEHIND ON SOCIAL MEDIA SECURITY



Social media manipulation is an important tool for malicious actors conducting influence activities against the interests of the Alliance.

In a 2019 report, the NATO StratCom CoE stress-tested a number of prominent platforms to determine their ability to identify and remove inauthentic accounts and content. By studying inauthentic accounts identified by purchasing around 50,000 fake engagements, the study concluded that the defences social media companies currently have in place are still woefully inadequate. [64] Therefore, we can continue to expect that antagonists will be able to exploit social media for malign purposes.

The Alliance must further refine its strategies for operating in a highly contested Information Environment. The ability to reduce the ability of antagonists to manipulate and exploit the information environment in times of crisis or war needs to be developed further.

Defend

Preventive measures must be paired with a strong defensive capacity to mitigate those incidents and attacks that do occur. Defensive capabilities should focus on setting up structures for active monitoring of the digital domain, and for working together to counter adversary activity.

Identify

Actively identify vulnerabilities.

Militaries should establish capabilities and procedures for active monitoring of the information environment in order to identify 1) ongoing attacks, 2) adversary preparations, and 3) their own vulnerabilities.

Armed forces should establish practices for monitoring the information environment at tactical, operational, and strategic levels.

In addition to adversary activities, these capacities should be focused on monitoring vulnerabilities in Allied forces and on OPSEC breaches in ongoing operations.

Monitored and unmonitored areas should be identified and then risks and vulnerabilities stemming from unmonitored areas (such as encrypted channels) should be assessed.

Situational awareness within the information environment needs to enable an analysis of what is not known as well as what is known to produce accurate assessments.

Cooperate

Cooperate with social media companies.

Allied armed forces should establish a mechanism to cooperate with social media companies and other digital service providers to improve measures that prevent, identify, analyse and counter the malicious use of digital information.

While these companies, in the light of recent developments, have implemented measures to better counter malicious activities and have responding to privacy and security concerns to some extent, substantial weaknesses still remain, which can have an impact on the outcomes of military operations.[65]

Engagement with social media companies could include an assessment of mutual vulnerabilities, information sharing/ reporting to liaison officers, and formalised cooperation to combat the malicious use of their environments.

Share information with capable partners

Allied armed forces should also establish a way of sharing information, for example with regard to identifying influence campaigns and those responsible for them, with relevant partners, domestic and foreign institutions, and the private sector.

Funding studies to identify, analyse, and counter risks in the information environment should be a priority in the coming years.

Counter

Develop the capacity to actively counter the malicious use of digital information.

Armed Forces in NATO countries should develop their capacity for actively countering the malicious use of digital information. Improvements in tactics, techniques, and procedures should encompass cyber, information, psychological, and kinetic operations.

Allied militaries should be able to:

- block/intercept the malicious use of digital information
- actively disrupt/shut down an adversary's digital intelligence networks through cyber or kinetic means
- recognise compromised digital information in a timely manner and adapt battlefield strategic, operational, and tactical planning (including troop deployment/position)
- influence social media and internet providers to limit opportunities for the malicious use of digital information (e.g. improved reporting of bot/troll activity and social engineering profiles/pages on social media)
- develop means of actively deceiving adversaries and camouflaging the activities of friendly troops in the digital information space.

Allied armed forces' updated capacities, tactics, techniques, and procedures for counter-activities should comply with ethical standards and with relevant domestic and international law. The *Tallinn Manual* on cyber warfare and operations can be a useful resource.[66] Responses will differ depending on operational environment, goals, and adversaries. Practices appropriate in peacetime will differ from those necessary for war/hybrid war scenarios.

FAMILIAR OPSEC COUNTERMEASURES...

'OPSEC measures protect critical information in one or more of the following ways: minimizing predictable patterns of behaviour; [avoiding] sudden changes to established routines [and in general any changes that] may alert an adversary to information about a mission; concealing indicators when they can't be avoided; [hiding] unusual activities or changes in routine by pairing them with meaningless changes; [and] providing an alternative interpretation for an indicator. An adversary can't make use of an indicator if he doesn't interpret it correctly.'[67]

...TRANSFORMED FOR THE DIGITAL DOMAIN

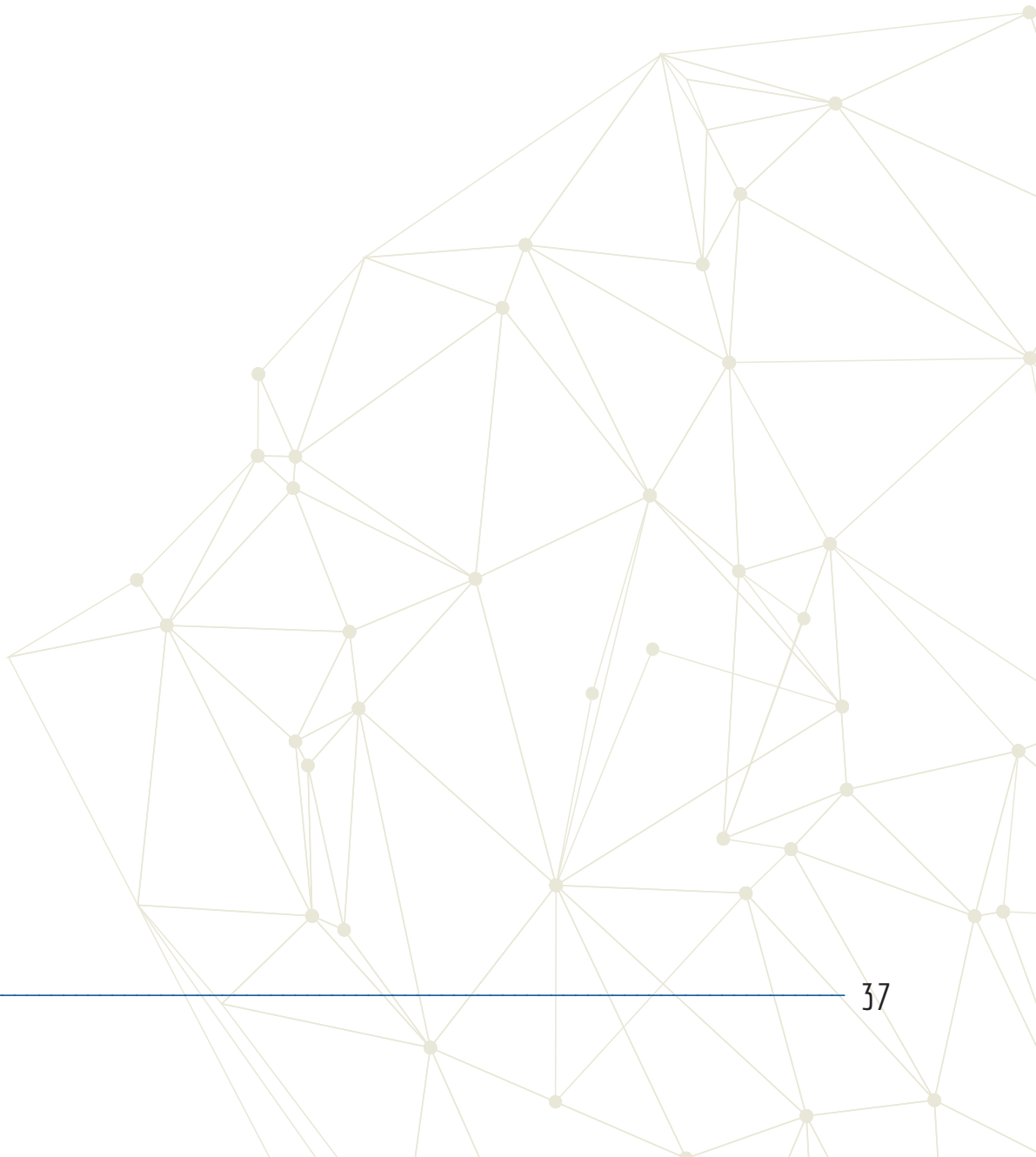
Evaluate

Conduct red-teaming to identify vulnerabilities.

Effective risk management and incident prevention rely on maintaining an adequate security posture. Regular and proactive evaluation is critical for the early discovery and mitigation of vulnerabilities.

For this purpose, the 'defender's mindset' constitutes one point of view. But there is also a need to look at one's own organisation 'through the eyes of the enemy' and mimic the thinking and actions of an attacker—this practice is commonly known as 'red teaming'.[68]

We recommend regular red-teaming exercises, combining cyber and influence activities, to be conducted against military units in order to raise awareness, to practice security and defence procedures, and to bolster resilience.



Key takeaways

Countering the malicious use of digital information is not simple, nor is it straightforward. As previous chapters have highlighted, armed forces and military organisations need to adopt new mind-sets as well as implementing a variety of activities to sufficiently safeguard against threats to force protection in the digital space. From our perspective, the following four key points are critical:

1. **Removing mobile phones is not enough**

   Removing mobile phones and other personal digital devices is critical for OPSEC in many contexts. Removing such devices, however, is not a complete remedy for the complex threats now inherent to the digital domain. In fact, removing phones creates new vulnerabilities because it lowers the threshold for malicious actors who seek to impersonate or otherwise influence the digital identities of military personnel by reducing own capacity to see what is happening in the digital space. Establishing a system of monitoring the digital identities of military personnel who are cut off from digital platforms for a longer period of time would mitigate this threat.

   The nature of conflict has changed—cyberthreat is ubiquitous. To deny military personnel access to the online environment for extended periods of time is unfeasible. Furthermore, digital data—including 'pattern-of-life' data—is continuously being collected. By the time a conflict arises, it might be too late for removing digital devices from armed forces personnel. Digital force protection needs to be continuous in both peace and war.

2. **Conduct red-teaming**

   Red-teaming threats in the information environment is essential for identifying risks and vulnerabilities at all levels—tactical, operational, and strategic. Given their evolving nature, commanders need to continuously develop their understanding of how such threats relate to their command.

   Methods for cybersecurity penetration testing can be used as a starting point for developing red-teaming methodologies, however the antagonist dimension of threats in the digital information space underscores the need for

dynamic red-teaming to accustom commanders to the dynamic and evolving nature of the threat.

3. **Train and exercise**

   Trainings concerning the malicious use of digital information should routinely be incorporated into military exercises, because this issue has tactical, operational, and strategic implications for any contemporary and future military operation. Neglecting to incorporate responding to digital threats and risks into military exercises is similar to training for winter warfare in the desert. 21st century conflicts are bound to be fought in, or near, digital and connected societies.

   Learning to effectively camouflage our troops, movements, and intents in the digital domain will be critical to mission success from here on out.

4. **Identify and counter**

   While camouflage in the digital domain will be critical to mission success, our ability to identify and counter ongoing digital reconnaissance and influence activities will be equally important.

   The ability to identify and counter hostile activities needs to be developed to support tactical and operational levels as well. A stray Instagram photo or a crowdsourcing campaign could have serious consequences in a conventional scenario.

   Beyond the risks associated with location, capabilities, and intent, significant risks are also associated with influence activities aimed at allied forces and neutral as well as hostile target audiences. Developing the ability to identify and counter influence activities needs to be prioritised in this field as well.

Conclusion

To ensure mission success for Allies and Partners, their adversaries' ability to maliciously exploit digital information must be limited. Force protection in the digital domain will be a decisive aspect in any future conflict.

There is an abundance of low-hanging fruit in this regard, where a small investment can pay large dividends. This report has highlighted the problem from a force protection perspective and has suggested potential measures military organisations could adopt to address the problem. These include identifying digital threats in the force protection process, educating soldiers and their families about digital security, and introducing friction related to digital information into military exercises. These activities can easily be implemented to improve our capacity to operate successfully in the contemporary battlespace.

However, these actions will not be sufficient to mitigate all risks in the digital domain. It is valuable to consider the force protection perspective, but without answers to broader cyber challenges on a more systemic level, military organisations will continue to be vulnerable. Camouflage is useful for concealment, but it is not a replacement for armour or offensive capabilities.

Sources

The British Army, 6th (United Kingdom) Division, 'Who we are?', *mod.gov.uk*, 2020.

Balkan, Serkan, DAESH's Drone Strategy: Technology and the Rise of Innovative Terrorism, (SETA, Foundation for Political, Economic and Social Research, 2017).

Bay, Sebastian, Georgio Bertolin, et al., Responding to Cognitive Security Challenges (Riga: NATO Strategic Communications Centre of Excellence, 2019).

Bay, Sebastian and Nora Biteniece, The Current Digital Arena and its Risks to Serving Military Personnel (Riga: NATO Strategic Communications Centre of Excellence, 2019).

Bay, Sebastian and Rolf Fredheim, Falling Behind: How Social Media Companies are Failing to Combat Inauthentic Behaviour Online (Riga: NATO Strategic Communications Centre of Excellence, 2019).

Bey, Sebastian (ed.) and Singularex, The Black Market for Social Media Manipulation, (Riga: NATO Strategic Communications Centre of Excellence, 2018).

Bellingcat, Posts tagged: MH-17, 2014–2019.

Bonnington, Christina, 'The Off-the-Grid Chat App That's Helping Hong Kong Protestors Organize' *Wired*, 2 October 2014.

Brangetto, Pascal, Emin Çalişkan, and Henry Rõigas, Cyber Red Teaming, (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015).

Brantly, Aaron and Muhammad Al-'Ubaydi, Extremist Forums Provide Digital OpSec Training. *CTC Sentinel,* Volume 8, Issue 5 (May 2015).

Brown, Daniel, 'Troops in Europe are jumping in lakes and wrapping their phones in condoms to thwart Russian hackers', *Business Insider*, 5 October 2017.

Brun, Itai, 'While You're Busy Making Other Plans' – The 'Other RMA', *Journal of Strategic Studies*, Volume 33, Issue 4, (2010): 535–65.

Cancian, Mark, 'Coping with Surprise in Great Power Conflicts', *Center for Strategic & International S*tudies, 20 February 2018.

Collins, Liam, 'Russia Gives Lessons in Electronic Warfare' *ARMY Magazine,* August 2018.

Cyber & Jihad Lab, 'Data Protection Guidelines in ISIS Weekly Encourage Readers To Use Encryption, Avoid Use Of Cellphones, Internet', *Memri*, 10 January 2019.

'Spårningen pågick – inne på Säpo', *Dagens Nyheter*, 25 April 2019.

Doffman, Zak, 'Cyber Warfare: Army Deploys "Social Media Warfare" Division to Fight Russia', *Forbes*, 1 August 2019.

Dreyfuss, Emily, 'Security News This Week: Telegram Says China Is Behind DDoS', *Wired*, 15 June 2019.

Gleicher, Nathaniel, 'Removing Coordinated Inauthentic Behavior from Iran, Russia, Macedonia and Kosovo', *Facebook Newsroom*, 26 March 2019.

Graham, Robert, 'How Terrorists Use Encryption', *CTC Sentinel,* Volume 9, Issue 6 (2016).

Greenberg, Andy, 'It Takes $1,000 to Track Someone's Location with Mobile Ads', *Wired*, 18 October 2017.

Grunt, Paweł, 'Structured Analytic Techniques: Taxonomy and Technique Selection for Information and Intelligence Analysis Practition', 2017.

Hackett, Robert, 'Cyber Saturday—Facebook's "War Room" Is a Marketing Ploy, *Fortune*, 21 October 2018.

Hern, Alex, 'Fitness Tracking App Strava Gives Away Location of Secret US Army Bases, *The Guardian*, 28 January 2018.

Horev, Rani, 'Style-based GANs – Generating and Tuning Realistic Artificial Faces' *LyrnAI*, 26 December 2018.

Horton, Michael, 'Fighting the Long War: The Evolution of al-Qa`ida in the Arabian Peninsula', *CTC Sentinel,* Volume 10, Issue 1 (2017).

Imperial College London, 'Anonymizing personal data 'not enough to protect privacy,' shows new study', *Techxplore*, 23 July 2019.

InformNapalm, Frequently Asked Questions, 7 August 2015.

InformNapalm, 'Syria. Kremlin's War Criminals – Infographics of Russian Air Force Officers' Disclosure', 27 October 2015.

Inform Napalm, 'SurkovLeaks (part 2): Hacktivsits publish new email dump', 03 November 2016.

InformNapalm, 'Who bombs civilians in Syria: profiles of 116 RuAF officers (Infographics)', 4 October 2016.

InformNapalm, ' "We're hauling tanks in from Anapa, from Temryuk," – Russian serviceman from 76th Maintenance Battalion testifies', 25 February 2019.

InformNapalm, 'Volunteers gathered evidence of 32 Russian military units taking part in the invasion of Crimea', 17 November 2019.

InformNapalm, About, 25 February 2020

Jackson, Brian A., David Frelinger, et al., 'Adaptation by Intelligent

Adversaries to Defensive Measures', *The Journal of Defense Modelling and Simulation*, 1 October 2018.

Katz, Or, 'Phishing Factories and Economies', *Akamai Security Intelligence & Threat Research*, 12 June 2019.

Kilcullen, David, Out of the Mountains: The Coming Age of the Urban Gorilla, (Oxford University Press, 2015).

Maxwell, Paul; Hall, Andrew and Daniel Bennet. ND. Cyber Operational Considerations in Dense Urban Terrain. *Small Wars Journal.*

Meyers, Adam, 'Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units', *Crowdstrike blog*, 22 December 2016.

Ministry of Defence, UK, 'Army restructures to confront evolving threats', *GOV.UK,* 31 July 2019.

Morgus, Robert and Justin Sherman, 'Analysis: Russia's Plans for a National Internet', *New America Cybersecurity Initiative blog*, 19 February 2019.

NATO, *Allied Joint Doctrine for Information Operations,* AJP-3.10, 2015.

NATO, *Summary note to Council on the Need to improve NATO's capability package process,* IBA-AR(2016)05, 2016.

NATO and UK Ministry of Defence, Allied Joint Doctrine for Force Protection AJP-3.14, NATO Standardization Office, April 2015.

NATO Science and Technology Board, STO Tech Trends Report 2017, (Brussels: NATO Science and Technology Organisation, 2017).

NATO Science and Technology Board, STO 2017 Highlights Report, (Brussels: NATO Science and Technology Organisation, 2018).

NATO StratCom CoE, About Strategic Communications, 2020.

NATO, *NATO Strategic Communication Policy*, 2009.

Newman, Lily Hay, 'What Spammers Could Do with Your Hacked Facebook Data' *Wired*, 19 October 2018.

Newton, Casey, 'The FBI wants to build a data dragnet on Facebook', *Verge*, 9 August 2019.

'OPSEC Awareness for Military Members, DoD Employees, and Contractors—Student Guide', Center for the Development of Security Excellence, ND.

Osborn, Andrew, 'Tinder, Despite Cooperation, Says It Hasn't Shared User Data with Russia Yet', *Reuters*, 3 June 2019.

Paul, Christopher, et al. *Improving C2 and Situational Awareness for Operations in and Through the Information Environment,* RAND, 2018

Petersen, Laura, et al., 'November 2015 Paris Terrorist Attacks and Social Media Use: Preliminary Findings from Authorities, Critical Infrastructure Operators and Journalists', ISCRAM 2018 Conference Proceedings, Rochester Institute of Technology, (2018): 629–38.

Perpet, Rosie, 'WhatsApp Disclosed 12 Security Flaws Last Year, Including 7 Classified as 'Critical', After Jeff Bezos Phone was Reportedly Hacked', *Business Insider*, 28 January 2020.

Press Trust of India, 'Kasab & co used VOIP during 26/11 attack', *India Times: The Economic Times*, 19 August 2009.

Riberio, John, 'Google Earth Used by Terrorists in India Attacks', *PC World*, 30 November 2008.

Riley-Smith, Tristram, 'Social Media in the Armed Forces', *Economic and Social Research Council*, October 2016.

Ross, Brian and James Gordon Meek, 'ISIS Threat at Home: FBI Warns US Military About Social Media Vulnerabilities', *ABC News*, 1 December 2014.

Nechepurenko, Ivan, 'Russia Votes to Ban Smartphone Use by Military, Trying to Hide Digital Traces', *New York Times*, 19 February 2019.

Schneier, Bruce, Click Here to Kill Everybody: Security and Survival in a Hyper-connected World (New York: W. W. Norton & Co., 2018).

Sherman, Justin, 'How to Regulate the Internet without Becoming a Dictator', *Foreign Policy*, 18 February 2019.

Simonite, Tom, 'The AI Text Generator That's Too Dangerous to Make Public, *Wired*, 14 February 2019.

Singer, Peter W. and Emerson T. Brooking, LikeWar: The Weaponization of Social Media, (New York: Houghton Mifflin Harcourt, 2018).

Sly, Liz, 'Inside an Undercover Network Trying to Expose Islamic State's Atrocities', *Washington Post*, 9 June 2015.

Stubbs, Jack, 'Factbox: Track Facebook's Fight Against Disinformation Campaigns in 2019', *Reuters*, 19 August 2019.

Supasorn Suwajanakorn, Steven M. Seitz, and Ira Kemelmacher-Shlizerman, 'Synthesizing Obama: Learning Lip Sync from Audio' *ACM Transactions on Graphics*, Article 95, Volume 36, № 4, (July 2017)

Tallinn Manual 2.0, (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2019).

Theonary, Catherine A., 'Information Warfare: Issues to Congress', *Congressional Research Service*, 5 March 2018.

Toler, Aric., 'Crowdsourced and Patriotic Digital Forensics in the Ukrainian Conflict' in Oliver Hahn and Florian Stalph (eds.), Digital Investigative Journalism: Data, Visual Analytics and Innovative Methodologies in International Reporting, (Palgrave Macmillan, 2018) p. 203.

Toler, Aric, 'Russia's "Anti-Selfie Soldier Law": Greatest Hits and Implications', *Bellingcat*, 20 February 2019.

Toler, Aric, 'Open Source Monitoring of NATO Trident Juncture Exercises' *Bellingcat*, 6 November 2018.

Travieso, Beatriz via Manuel Cebrian, 'Crowdsourcing Search: The Red Balloon Challenge', MIT Media Lab, Project active January 2010 to September 2014.

Ünver, H. Akın, 'Digital Open Source Intelligence and International Security: A Primer', *Cyber Governance and Digital Democracy 2108/8*, EDAM, Oxford CTGA & Kadir Has Üniversites.

Willemo, Jakob, Trends and Developments in Malicious Use of Social Media, (Riga: NATO Strategic Communications Centre of Excellence, 2019).

Zargham, Mohammad, 'Pentagon Restricts use of Geolocation Software for Troops', Reuters, 2018.

Endnotes

1 Sebastian Bay and Nora Biteniece, The Current Digital Arena And Its Risks To Serving Military Personnel, (Riga: NATO Strategic Communications Centre of Excellence, 2019).
2 Brian Ross and James Gordon Meek, 'ISIS Threat at Home: FBI Warns US Military About Social Media Vulnerabilities', ABC News, 1 December 2014.
3 Aric Toler, 'Russia's "Anti-Selfie Soldier Law": Greatest Hits and Implication', Bellingcat, 20 February 2019.
4 Alex Hern, 'Fitness tracking app Strava gives away location of secret US army bases', The Guardian, 29 January 2018.
5 'Spårningen pågick – inne på Säpo', Dagens Nyheter, 25 April 2019.
6 Bay and Biteniece, The Current Digital Arena.
7 Author's interview with researchers at Tallinn Technical University, spring 2019.
8 Red-teaming refers to the practise of systematically challenging plans, policies, approaches, assumptions or systems by adopting an adversarial approach. The purpose of red-teaming is to mitigate bias and encourage consideration of adversarial perspectives. The practise is often used by military organisations as a Structured Analysis Technique (SAT). For more, see Paweł Grunt, Structured Analytic Techniques: Taxonomy and Technique Selection for Information and Intelligence Analysis Practition, 2017.
9 Author's interview with participants of the red-team, 2016.
10 Allied Joint Doctrine for Force Protection AJP-3.14 with UK National Elements, UK Ministry of Defence and NATO Standardization Office, April 2015.
11 Aric Toler, 'Crowdsourced and Patriotic Digital Forensics in the Ukrainian Conflict' in Oliver Hahn and Florian Stalph (eds.), Digital Investigative Journalism: Data, Visual Analytics and Innovative Methodologies in International Reporting, (Palgrave Macmillan, 2018) p. 203.
12 Black markets with products 'as-a-service' exist for virtually any type of malicious online action. Sebastian Bey (ed.) and Singularex, The Black Market for Social Media Manipulation, (Riga: NATO Strategic Communications Centre of Excellence, 2018); Or Katz, 'Phishing Factories and Economies', Akamai Security Intelligence & Threat Research, 12 June 2019.
13 Succinctly expressed: 'All this means that expertise flows downhill. Yesterday's top-secret military capabilities become today's PhD theses and tomorrow's hacking tools.' Bruce Schneier, Click Here to Kill Everybody: Security and Survival in a Hyper-connected World (New York: W. W. Norton & Co., 2018) p. 32.
14 The hacking of Amazon COE Jeff Bezos' phone in November 2018 though a security flaw in popular Facebook-owned messaging app WhatsApp has furthered customer concern for privacy. See Rosie Perper, 'WhatsApp disclosed 12 security flaws last year, including 7 classified as 'critical', after Jeff Bezos phone was reportedly hacked', Business Insider, 28 January 2020.
15 Jakob Willemo, Trends and Developments in Malicious Use of Social Media (Riga: NATO STRATCOM COE, 2019) p. 1; Aaron Brantly and Muhammad Al-'Ubaydi, 'Extremist Forums Provide Digital OpSec Training', CTC Sentinel, Volume 8, Issue 5, May 2015.
16 Interview with Dave Bittner and Joseph Carrigan in Willemo, Trends and Developments, p. 3–4; for information on deepfakes, see Rani Horev, 'Style-based GANs—Generating and Tuning Realistic Artificial Faces', LyrnAI, 26 December 2018; Supasorn Suwajanakorn, Steven M. Seitz, and Ira Kemelmacher-Shlizerman, 'Synthesizing Obama: Learning Lip Sync from Audio' ACM Transactions on Graphics, Article 95, Volume 36, № 4, (July 2017); Tom Simonite, 'The AI Text Generator That's Too Dangerous to Make Public', Wired 14 February 2019.
17 NATO Science and Technology Board, Tech Trends Report 2017, (Brussels: NATO Science and Technology Organisation, 2017) p. 13.
18 Schneier, Click Here to Kill Everybody, p. 174.
19 See the entire archive of Bellingcat's coverage of the downing of flight MH-17, Posts tagged: MH-17, 2014–19.
20 Aric Toler, 'Russia's "Anti-Selfie Soldier Law": Greatest Hits and Implications' Bellingcat, 20 February 2019.
21 Ibid.
22 Beatriz Travieso via Manuel Cebrian, 'Crowdsourcing Search: The Red Balloon Challenge', MIT Media Lab, Project active January 2010 to September 2014.
23 Andy Greenberg, 'It Takes $1,000 to track Someone's Location with Mobile Ads', Wired, 18 October 2017.
24 Spårningen pågick, Dagens Nyheter.
25 Frequently Asked Questions. InformNapalm, 7 August 2015.
26 Serkan Balkan, DAESH's Drone Strategy: Technology and the Rise of Innovative Terrorism, (Istanbul: SETA Foundation for Political, Economic and Social Research, 2017)
27 See Case Study Box—Neptune 2018 below.
28 Plane- and ship-spotters are individuals who voluntarily report on the locations of planes and ships they observe.
29 Aric Toler, 'Open Source Monitoring of NATO Trident Juncture Exercises', Bellingcat, 6 November 2018.
30 Ibid.

31 PO(2011)0210 c.f. NATO Summary note to Council on the Need to improve NATO's capability package process, IBA-AR(2016)05, 2016
32 David Kilcullen, Out of the Mountains: The Coming Age of the Urban Gorilla, (Oxford University Press, 2015).
33 John Riberio, 'Google Earth Used by Terrorists in India Attacks', PC World, 30 November 2008.
34 Press Trust of India, 'Kasab & co used VOIP during 26/11 attack', India Times: The Economic Times, 19 August 2009.
35 Emily Dreyfuss, 'Security News This Week: Telegram Says China Is Behind DDoS' Wired, 15 June 2019.
36 Christina Bonnington, 'The Off-the-Grid Chat App That's Helping Hong Kong Protestors Organize', Wired, 2 October 2014.
37 Author's interviews with exercise participants, spring 2019.
38 Interview with research team, April 2019.
39 InformNapalm, About, 25 February 2020
40 InformNapalm, 'SurkovLeaks (part 2): Hacktivsits publish new email dump', 03 November 2016.
41 InformNapalm, 'Volunteers gathered evidence of 32 Russian military units taking part in the invasion of Crimea', 17 November 2019.
42 InformNapalm, 'Syria. Kremlin's War Criminals – Infographics of Russian Air Force Officers' Disclosure', 27 October 2015.
43 Paul, et al. Improving C2 and Situational Awareness for Operations in and Through the Information Environment, RAND, 2018
44 Extrapolated from NATO's conception of information activities in NATO, Allied Joint Doctrine for Information Operations AJP-3.10, 2015.
45 Bay and Biteniece, The Current Digital Arena.
46 Ibid.
47 NATO Science and Technology Organization, Social Media Exploitation for Operations in the Information Environment, (To be published).
48 For examples from the US Army Training and Doctrine Command Mad Scientist Initiative see Paul Maxwell, Andrew Hall and Daniel Bennet, 'Cyber Operational Considerations in Dense Urban Terrain' Small Wars Journal, ND.
49 Itai Brun, 'While You're Busy Making Other Plans' – The 'Other RMA', Journal of Strategic Studies, Vol. 33, Iss. 4, (2010): 535–65.
50 Ivan Nechepurenko, 'Russia Votes to Ban Smartphone Use by Military, Trying to Hide Digital Traces', New York Times, 19 February 2019.
51 Liam Collins, 'Russia Gives Lessons in Electronic Warfare', ARMY Magazine, August 2018, p. 18–19.
52 Brantly and Al-'Ubaydi, 'Extremist Forums Provide Digital OpSec Training'.
53 Brian A. Jackson, David Frelinger, et al. 'Adaptation by Intelligent Adversaries to Defensive Measures', The Journal of Defense Modelling and Simulation, 1 October 2018
54 For example, the citizen journalist group Raqqa Is Being Slaughtered Silently published first-hand accounts from one of the most restricted areas of Syrian civil war. They did their reporting under threat of torture or death by militants from the so-called Islamic state.
55 H. Akın Ünver, 'Digital Open Source Intelligence and International Security: A Primer', Cyber Governance and Digital Democracy, Volume 8 (2018).
56 Doxing refers to the internet-based practice of collecting and publishing private information about an individual or an organization.
57 Collins, Russia Gives Lessons in Electronic Warfare; Cancian, Coping with Surprise, p. 66.
58 Ibid.
59 Bittner and Carrigan in Willemo, Trends and Developments, p.7.
60 Adam Meyers, 'Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units', Crowdstrike blog, 22 December 2016.
61 NATO StratCom CoE website, 'About Strategic Communications'.
62 NATO Strategic Communications Policy, 2009
63 Lily Hay Newman, 'What Spammers Could Do with Your Hacked Facebook Data', Wired, 19 October 2018.
64 Sebastian Bay and Rolf Fredheim, Falling Behind: How Social Media Companies are Failing to Combat Inauthentic Behaviour Online (Riga: NATO Strategic Communications Centre of Excellence, 2019).
65 Bay and Fredheim, Falling Behind.
66 Tallinn Manual 2.0, (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2019).
67 'OPSEC Awareness for Military Members, DoD Employees, and Contractors—Student Guide', Center for the Development of Security Excellence, ND.
68 Pascal Brangetto, Emin Çalişkan, and Henry Rõigas, Cyber Red Teaming (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015).

Prepared and published by the
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

The NATO Strategic Communications Centre of Excellence (NATO StratCom COE) is a NATO accredited multi-national organisation that conducts research, publishes studies, and provides strategic communications training for government and military personnel. Our mission is to make a positive contribution to Alliance's understanding of strategic communications and to facilitate accurate, appropriate, and timely communication among its members as objectives and roles emerge and evolve in the rapidly changing information environment.

Operating since 2014, we have carried out significant research enhancing NATO nations' situational awareness of the information environment and have contributed to exercises and trainings with subject matter expertise.

www.stratcomcoe.org | @stratcomcoe | info@stratcomcoe.org