ISBN: 978-9934-564-39-0

RESPONDING TO COGNITIVE SECURITY CHALLENGES

THE CURRENT DIGITAL ARENA AND ITS RISKS TO SERVING MILITARY PERSONNEL

Sebastian Bay, Nora Biteniece

This article is published as a part of a study "Responding to Cognitive Security Challenges". Full report is also available online: www.stratcomcoe.org

ISBN: 978-9934-564-39-0
Authors: Sebastian Bay, Giorgio Bertolin, Nora Biteniece, Edward H. Christie, Anton Dek, Rolf E. Fredheim, John D. Gallacher, Kateryna Kononova, Tetiana Marchenko
Project manager: Giorgio Bertolin
Text editor: Anna Reynolds, Mike Collier
Design: Kārlis Ulmanis

Riga, January 2019
NATO STRATCOM COE
11b Kalciema Iela
Riga LV1048, Latvia
www.stratcomcoe.org
Facebook/stratcomcoe
Twitter: @stratcomcoe

02

THE CURRENT DIGITAL ARENA AND ITS RISKS TO SERVING MILITARY PERSONNEL

Sebastian Bay, Nora Biteniece

ABSTRACT

The last few years have provided an abundance of examples of how malicious actors can exploit user data to the detriment of social media users, armed forces, and society. This study explores what kind of user data is available in the digital environment and demonstrates how a malicious actor can exploit this data in the context of a military exercise. The results of an experiment conducted by a NATO StratCom COE research team suggest that in the current digital arena an adversary would be able to collect enough personal data on soldiers to create targeted messages with precision, successfully influencing their chosen target audience to carry out desired behaviours.

INTRODUCTION

In the wake of the Cambridge Analytica scandal, the broad media coverage of Facebook CEO Mark Zuckerberg's appearance before the US Congress, and the implementation of the General Data Protection Regulation (GDPR) in the European Union, the news-watching public is becoming increasingly aware that data is constantly being collected about virtually every aspect of our digital lives.

Whenever we browse the internet, purchase goods online, move around the world with our smartphones, or interact with our peers, we generate large amounts of data that are collected by social media companies, internet service providers, and data brokers. With the advent of Internet of Things (IoT), data is now also being collected about our health, our homes, our pets, as well as about our digital equipment and how we use it. The International Data Corporation (IDC) forecasts that by 2025 annual global data creation will have grown tenfold to 163 zettabytes.[1,2]

Cambridge Analytica allegedly analysed thousands of data points on hundreds of millions of Americans to generate effective microtargeting and behaviour-prediction algorithms during the 2016 US presidential election campaign. In light of these events, it is imperative that we increase our understanding of the possibilities for malicious use of data.[3] Much of the data used by Cambridge Analytica was collected

> Data is now also being collected about our health, our homes, our pets, as well as about our digital equipment and how we use it. Malicious use of data: the usage of data exploiting vulnerabilities in order to deceive, disrupt, interfere and ultimately do harm to individuals and/or society.

using the Facebook app 'This is Your Digital Life'. Roughly 270,000 people used this app and unwittingly shared their personal data, and that of their friends, with Cambridge Analytica. It has been estimated that the personal information of roughly 50 million Americans was harvested this way.[4] And Cambridge Analytica is not the only company collecting data on private citizens. Data has become an important component of our digital existence because people now expect customised search results and an online experience tailored to their personal needs, wants, and desires. This kind of customisation is not possible without extensive data collection.

In his testimony to Congress in April 2018, Facebook CEO Mark Zuckerberg described the data Facebook collects on its users as 'information people choose to share online' and 'data needed to make ads relevant'.[5] However, this description leaves out two kinds of data — the metadata users share involuntarily (online behaviour, personal activities, type of hardware used) and data derived, inferred, or predicted from the data shared and generated by users. These kinds of data can reveal surprising insights about both individuals and groups. In simple terms, information about the things users post and like online, combined with where they are, how they travel, and which devices and apps they use, can be used to make predictions about individuals gender, sexual orientation, political leanings, personality, and other characteristics that define us as people.[6,7] Facebook also uses metadata, such as device model, whether they are using WiFi or have been travelling abroad, to add users to categories advertising clients can use to target the users. Facebook also infers characteristics, such as 'potentially interested in switching mobile carrier', from this metadata. A malicious actor could potentially combine an inferred trait

such as 'potentially interested in switching mobile carrier' with provided data such as listed employer e.g., 'Country X Armed Forces' to target specific users much more effectively.

Although many know that their online presence leaves many digital traces, far fewer are aware that by using various combinations of data (such as calls, SMS, Bluetooth, and app usage) researchers have been able to predict users' 'Big Five' personality traits (openness, conscientiousness, extraversion, agreeableness, neuroticism) to model personality/psychopathology.[8] Indeed, knowledge of any four apps installed on a person's smartphone has proven enough to identify 95% of users in a given data set.[9,10,11]

This report discusses what kind of user data is available in the digital environment, and how a malicious actor might exploit this data. In this report "malicious use of data" refers to the usage of data exploiting vulnerabilities in order to deceive, disrupt, interfere and ultimately do harm to individuals and/or society. In assessing if the usage of data is malicious, we have based our discussions on the DIDI-model[12] proposed by Pammet at al., for diagnosing illegitimate influence.[13]

In this report we also present the results of an experiment conducted by the NATO Strategic Communications Centre of Excellence to discover how a malicious actor might exploit user data within the context of a national military exercise.

What kind of user data is available?

Data brokers, such as Acxiom and Epsilon, have grown into multibillion-dollar companies that make a living out of collecting and reselling data.

Data brokers do one of three things:

1) search for information about individuals (name address, income, debt, family)[14] develop dossiers on individuals (age, demographics, family, interests, contact information, health information, etc.);[15]

2) group individuals into segments marketers can use for targeted advertisements;

3) gather information to verify identities and assess risk (often financial risk).[16] Data brokers combine data they have collected with social media data, i.e., user actions (such as providing gender, age, and location), and user interactions on social media platforms (such as liking posts, joining groups, and using a specific device), to create custom segments or detailed digital portraits of targeted individuals and groups.[17]

Social media companies allow advertisers to target their users by uploading custom audience sets, enabling advertisers to use outside datasets (e.g. subscribers to an email list or a contact list of individuals who have recently bought a certain item)

We have reached a point where it is no longer possible to have a complete overview of the data we use and generate.

to target ads to individuals on the social media. The resulting list (e.g. people who have bought a certain item and use a specific social media platform) can then be further refined using additional data derived from the social media platforms. The result is a highly customised datasets enabling unprecedented microtargeting of social media users.[18] Recent developments have pushed social media companies to limit the use and abuse of ads targeted based on psychographics visible to individual users (also known as 'dark ads')[19], and third-party data,[20] but so far most companies still allow the use of third-party data for targeting ads on their platforms. Social media companies also use third-party data to track and measure ads and ad engagement criteria, such as sales and sentiment.

We have reached a point where it is no longer possible to have a complete overview of the data we use and generate. The number of data points available on any one individual cannot be counted, as they are created and re-created non-stop. Public government data, social media data, and commercial data, together with data aggregated and inferred from these records, create enormous amounts of data with unimaginable scope. This does not mean that comprehensive data is available about every individual, but it does mean that ad targeting is gradually becoming more and more precise, creating unprecedented possibilities for the use and abuse of data.

How can data be used in a malicious way?

The malicious use of data is a more serious problem than targeted messaging. The collection and use of personal data for criminal objectives can have consequences that go far beyond influencing the behaviour of potential customers. Below we identify some of these risks associated with data collection and analysis, taking into consideration the information security principles of confidentiality, availability, and integrity.

MALICIOUS WAYS

Manipulation

A diverse range of industries — from finance and insurance to health and migration — collect data to make business decisions. Since most people usually aren't aware this data about them exists, or what kinds of decisions are being made based on this data, there is a risk that inaccurate data could have severe consequences for individuals without their knowledge.[31] For example, inaccurate data could prevent a person from securing a loan or being granted a security clearance. Inaccurate data can cause an organisation to make erroneous decisions and lost data can be difficult or expensive to replace.

Impersonation

Access to personal information makes it easier for malicious actors to impersonate people online. Personal information can also be used to predict passwords and answer security questions in order to gain access to accounts, and to convince companies and government entities to take specific actions. The confidentiality of personal data is essential for the proper functioning of authorisation layers that control access to sensitive information.

Doxing

Doxing is the technique of intentionally releasing selected information about an individual to influence public perception of that individual, or the creation of conditions and vulnerabilities that can be exploited. The confidentiality of information safeguards the credibility of both individuals and organisations.

Sensitive information

Data generated by our devices, particularly by our mobile devices, often reveal sensitive information about the locations and activities of the people using them. During the Russian annexation and occupation of Crimea and Eastern Ukraine, Russian soldiers and civilians shared a wealth of information that made it possible to verify Russian aggression in Ukraine. The open source verification organisation Bellingcat was able to determine precisely how a Buk missile launcher reached a particular field in eastern Ukraine, who organised the transport, where the missile launcher came from before it arrived in Ukraine, and even identify the (near-complete) history of a single launch unit. However, advances in this area also provide opportunities for malicious actors to exploit data leakage, creating new risk in the military domain.

EXPERIMENTATION

A research team from NATO Strategic Communications Centre of Excellence conducted an experiment in support of a military exercise in an Allied country. We embedded a research team within a red-team cell[21] to evaluate how much data we could collect about exercise participants, to test different open-source intelligence techniques, and to determine if we would be able to induce certain behaviours such as leaving their positions, not fulfilling duties, etc. using a range of influence activities based on the acquired data.

The research team collected open source data during a military exercise targeting armed forces personnel. To protect the privacy of those taking part in the military exercise, no personal data identified during the experiment was stored.[22] The experiment focused on the active phase of the military exercise. The preparations made by the research team took three to four weeks; these included planning the operation, setting up the necessary online accounts, assessing the online information environment, and creating a range of messages and lines of persuasion. The scope of the experiment was limited in comparison to large-scale efforts such as the work undertaken by the Kremlin's Internet Research Agency to influence the US presidential election 2016. An operation of that scale requires months of preparation to set up the necessary infrastructure and develop quality target audience analysis.[23]

Methodology

To assess the extent to which we would be able to exploit social media and open source data to gather information on and influence military personnel during a military exercise, the research team used:

- Impersonation[24]
- Honeypot pages[25]
- Social engineering[26]
- General monitoring and befriending of accounts
- Peoples search engines[27] and open source databases

The level of personal information that could be found using the above methods was very detailed and enabled the research teams to craft influence activities. Information about the exercise itself was found both from exercise participants and public sources such as news and official armed forces pages.

We monitored exercise participants using their Facebook, Instagram, and Twitter accounts. These platforms provided the research team with access to basic information about their targets as they allow users to search by name/username and view any information that has been made public by the platform users.

”The level of personal information we found was very detailed and enabled us to instil undesirable behaviour during the exercise.

Results and Findings

The methods employed by the research team resulted in honeypot pages and groups being liked and joined by exercise participants. Shortly after the groups were created and promoted, Facebook shut down the honeypot pages,[28] which meant that the audience acquired through Facebook Ads was lost, and researchers could no longer advertise exclusively to followers of the honeypot pages.

The members of the closed groups were used as a starting point to gather more information. As described in the previous section, researchers searched for information about their targets in public sources, monitored their social media accounts, and attempted to engage them directly via group discussions and messages. The exact methods and their success cannot be disclosed due to operation security.

Overall, we identified a significant amount of people taking part in the exercise and managed to identify all members of certain units, pinpoint the exact locations of several battalions, gain knowledge of troop movements to and from exercises, and discover the dates of the active phases of the exercise. The level of personal information we found was very detailed and enabled us to instil undesirable behaviour during the exercise.

We found that Instagram was popular among soldiers during the exercise, and therefore provided the timeliest information. Facebook, by comparison, was a good starting point for identifying individuals and for mapping their links to other members of the armed forces using the suggested friends feature.[29] Twitter was rarely used during the exercise, and gave no useful information.

The soldiers who were targeted using social engineering shared more information with researchers than the information that could be found about them on their social media accounts. We managed to get an approximate location (+/-1km) for exercise participants, including soldiers from high value units, i.e., units that were required to complete a mission. We obtained phone numbers, email addresses, and pictures of equipment from all participants targeted using social engineering.

Social Media Countermeasures

An important part of our experiment involved the creation of honeypot pages, groups, and profiles on social media to gather data and to test the countermeasures of social media companies. During the exercise, we created honeypot Facebook pages that published information from other sources regarding the exercise, and Facebook pages impersonating the official armed forces page. In addition, we created several social media accounts. Four accounts impersonated real people from the armed forces and one account was entirely fake. The social media companies deployed counter measures to counter our abuse of their platforms with varying degrees of success.

The table below summarises the social media countermeasures we experienced during this process:

Type	Uptime	Cause
Honeypot pages	2 weeks	Reported to Facebook
Pages impersonating existing page	Suspended after 1–2 hours	Did not comply with Facebook T&C
Closed groups	Never suspended	
Fake profile	Never suspended	
Profiles impersonating real people	From 2 hours to infinite Two profiles suspended after 2 hours One profile suspended after one day One profile was never suspended	Reported to Facebook Suspicious activity detected by Facebook

Social Media Vulnerabilities

Prior to the experiment, we found that Facebook only partially respects the privacy settings for workplace disclosure. Accounts that did not publicly display their workplace, still appeared in results when searching for employees using a certain Facebook feature. The security team at Facebook has been informed about this "bug".

We also noticed several profiles that were clearly fake, or not related to the target country in any way, which listed the armed

> The privacy features and settings of social media platforms cannot be trusted not to leak information to other layers of the social media platform.

forces targeted by the research team as their workplace. This is a potential vulnerability that malicious actors can exploit — private accounts are allowed to list any entity as employer, which creates a situation whereby accounts can choose to intercept public information intended only for a certain group. There is no simple solution to this problem, as a new set of security challenges would stem from attempts to ensure that only actual employees are able to declare a particular place of work on their Facebook profiles.

Both of these vulnerabilities underscore one important thing — the privacy features and settings of social media platforms cannot be trusted not to leak information to other layers of the social media platform, or to other users and companies with an interest in such information.

CONCLUSIONS

In an essay entitled Preparing for Elections, Facebook CEO Mark Zuckerberg stated that his focus for 2018 is to defend elections against interference, protect the community from abuse, and make sure individuals have more control of their information.[30] These are all important and complex steps that must to be taken by all responsible and serious actors. After years of social media manipulation by malicious actors, we finally have movement in the right direction.

However, states and its citizens need more than verbal assurances that our vital assets will be protected. We must probe, test, and continuously evaluate how data exploitation by malicious actors can threaten allied goals and interests. We need to build not only an infrastructure that protects us, but also improve the training and exercises that test our ability to detect and counter influence activities.

Our 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 this data can be used to target messages with precision, successfully influencing members of the target audience to carry out desired behaviours.

However, although we managed to collect data and induce behaviour detrimental to the conduct of military operations, we also faced a number of difficulties indicating that social media companies are increasing their efforts to prevent abuse of their platforms. Facebook in particular provided significant pushback, and several of our fake accounts and pages were suspended during the course of the experiment. The fact that social media abuse has been much debated as a phenomenon during the last year has increased public and institutional awareness of the risks and challenges. The effect of this heightened sensitivity was that several of our fake profiles and pages were reported by the armed forces we targeted, and on one occasion a warning for the fake page we had created was circulated.

Even so, despite heightened sensitivity and active users reporting suspicious behaviour, we were successful on a number of occasions, proving that misuse of social media platforms for targeting purposes is still quite possible. Our experiment showed that much remains to be done to improve security, both by the social media companies and by the armed forces. Some of the flaws that enabled us to manipulate social media and social media users are human flaws that can only be addressed through better training and stricter control. But other flaws, such as the lack of transparency, opportunities for microtargeting, and misuse of anonymity, are vulnerabilities built into the social media platforms themselves; this highlights the continuing need to improve these platforms. Two immediate changes that the social media platforms should consider in order to reduce vulnerabilities are:

- Stricter control of the 'suggested friends' feature – a friend should not be suggested unless the user has accepted the friend request. As it stands now, this feature made it extremely easy for us to map out entire units and battalions by identifying only a single member of a unit.

- Preventing search features to showing hidden data – searches should not be allowed to show results that have intentionally been hidden from the public profile by the users.

Our final conclusion is an old conclusion that bears repeating. The armed forces must step up monitoring and countermeasures to reduce the risk of social media being used to gather mission-sensitive information. This is, and will continue to be, a significant challenge in the years to come.