H. Rossnagel, C.H. Schunk, S. Mödersheim, D. Hühnlein (Hrsg.): Open Identity Summit 2020,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020 61

Identity Management as a target in cyberwar

Lothar Fritsch[1]

Abstract: This article will discuss Identity Management (IdM) and digital identities in the context of cyberwar. Cyberattacks that target or exploit digital identities in this context gain leverage through the central position of IdM digital infrastructures. Such attacks will compromize service operations, reduce the security of citizens and will expose personal data - those of military personell included. The article defines the issue, summarizes its background and then discusses the implications of cyberwar for vendors and applicants digital identity management infrastructures where IdM is positioned as a critical infrastructure in society.

Keywords: Identity management; Cyberwar; Cyber conflict; Digital identities; Information Privacy; Critical Infrastructure Protection; Security; Cyberconflict; Cybersecurity

```
"The events which can not be prevented, must be directed."
- Klemens von Metternich
```

1 Introduction

Identity management is a technological platform that enables the identification and verification of persons or computers as well as the processing of persons, of ownership over physical or virtual objects and over all other imaginable resources. Mobile phone subscriptions and bank accounts as well as payment systems are well-known domains where IdM plays a critical role. Less visible domains are public utilities, government administration or health services, where in progressing digitization of services IdM is introduced to both control access and roles of employees as well as to identify persons who are being administered, billed or privileged through IdM.

IdM is therefore a critical infrastructure that underlies many other of society's critical infrastructures and functions, while making citizens involuntarily accessible to external actors [HG08]. This article will discuss Identity Management as a critical asset in the context of cyberwar. It will discuss the relevance in face of power and military action, then illustrate the issue with examples. Digital identity will be positioned as an attack vector for

[1] Karlstad University, Dept. of Mathematics and Computer Science, Universitetsgatan 2, Karlstad, Sweden
lothar.fritsch@kau.se emailaddress@author2

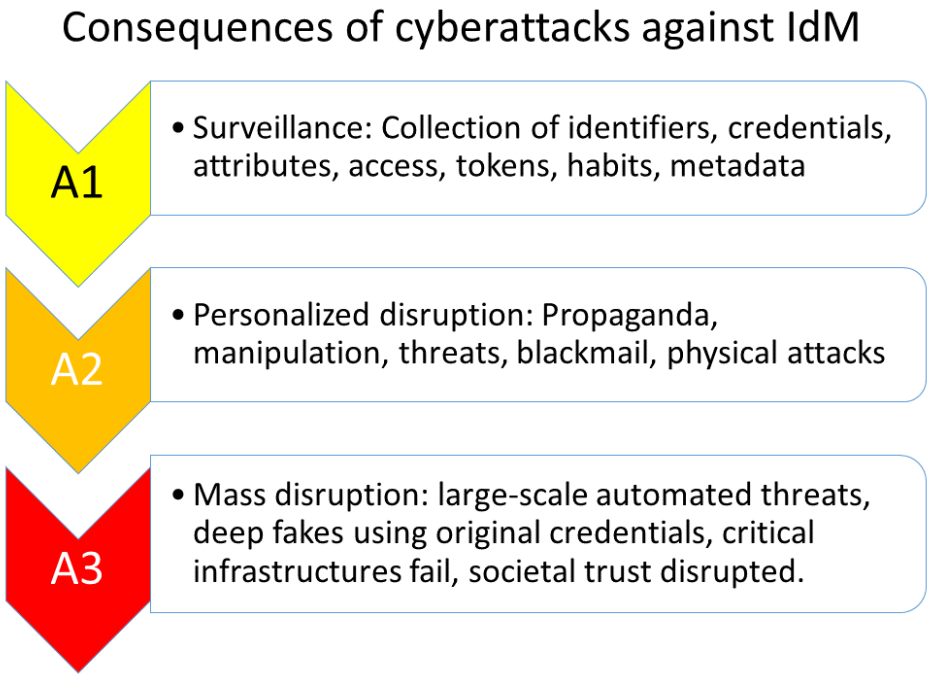

Fig. 1: Consequences of three escalating categories A1,A2 and A3 of cyberattacks on identity management.

cyberattacks. Next, possible regulatory restrictions will be introduced, before I conclude and summarize.

The main argument of this article is:
IdM ist the key to most digital environments, the key to all citizens (military and civil), and has therefore major relevance in national security and sovereignty in the context of cyberwar.

2 Background

IdM is of major relevance in the national security context. First, it enables the governance of digital services of all kinds, and is therefore a part of most digital civil, administrative and critical infrastructures, including communications. Next, digital identities are directly associated with individuals, which turns them into tools to track, profile, find and access those people. Third, digital identities are used directly in military contexts where they are the key to personnel, equipment or actions. The role of RFID auto-identification of goods and products in industrial espionage and sabotage has been illustrated by Fritsch in

[Fr09]. The remainder of this section will discuss examples of how IdM is closely related to cybersecurity, and how compromize of digital identities endangers societal security and sovereignty.

Digital identities can get exploited for various adverse actions in escalating levels of impact on societal security (labeled as categories A1-A3 below):

A1: Surveillance and intelligence gathering: Key persons or large segments of populations can be targeted through digital identities for observation.

A2: Personalized manipulation and disruption: Through individual digital identities, people can be targeted for influence campaigns or can become the individual target of adverse action.

A3: Mass exploitation or disruption of services: Compromize of IdM at a large scale will enable the disruption of critical societal functions, either through their simple destruction that will render identification as well as archives useless, or through targeted exploitation of stolen identities for disruptive actions that target society's critical processes and services.

The consequences of these actions are llustrated in Fig. 1. It is noteworthy that digital identities bridge from the digital into the physical domain. Cyberattacks may combine into cyberphysical attacks where digital surveillance from A1 may lead to physical action against persons in A2 and A3. Fig. 2 illustrates how digital identifiers connect digital and physical spaces in ways that are exploitable by attackers even in the physical domain.

Simple observation of digital identities can leak critical secrets. In 2018, a fitness app for self-metering of jogging performance published trail maps of joggers that were found to reveal secret military facilities used by U.S. troops [2].Such data extraction relates to category A1. Further investigation of fitness apps' data extraction confirmed how unverified apps can easily access critical identities and personal data [MHF19].

Kallberg [Ka16] discusses pillars of societal stability that will be at risk through cyber attacks (pp. 121). Cyberwar strategy aims at the destabilization of the target contry's functioning institutional arrangements. He explicitly discusses governmental registers and archives with institutional knowledge such as property registers as potential targets. The pivotal role of IdM in governance puts IdM in the core of such attack strategies. Such actions fall into category A3.

Dunlap [Du14] discusses the consequences of a future hyperpersonalization of war through digital identities. Dunlap reasons about digital technologies as enablers of acts of war that target specific individuals. He describes two relevant cases which are in category A2:

[2] The Guardian: Fitness tracking app Strava gives away location of secret US army bases, 2018-01-28, https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases , accessed 2020-02-21

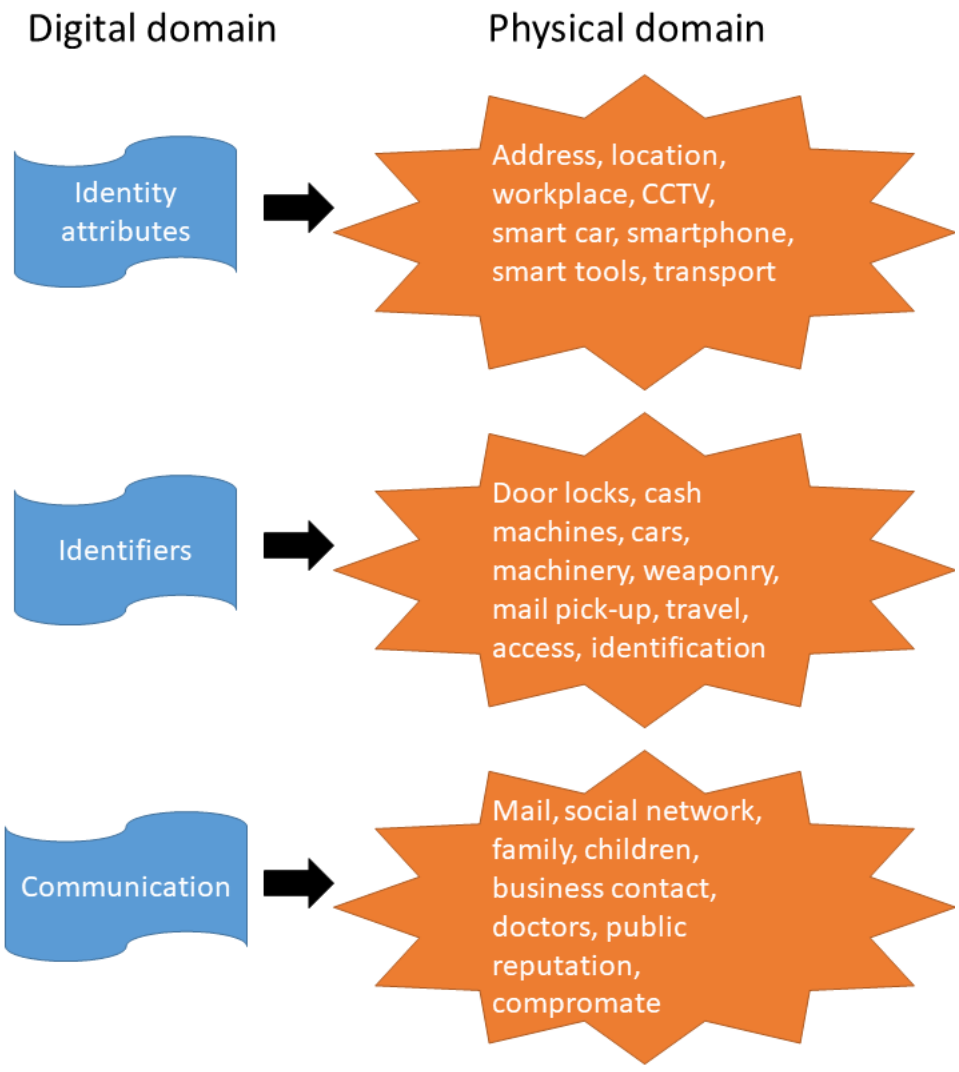

Fig. 2: Identity management causes cyberphysical security and privacy problems when exploited in cyberwar.

1. The targeting of individual soldiers with biometrics-enabled or otherwise personalized weapons.This vision is illustrated by the short film *Slaughterbots* [3]. Similar tactics have already historically been observed being used against U.S. soldiers in the Pacific who found their private browser history published on the Internet [4]. Similar threats have been addressed to U.S. soldier's smart phones in 2019 [5]. Worries about digital targeting have been voiced by Swedish defense researchers Sigholm and Andersson [SA11] who reason about future battlefield technology's exposing of soldier's personal data. Case examples from the Iraq war have been collected by Conti et al. [Co10] who documented the naive use of identifiers in battlefield. Personal data gets weaponized in conflicts. This problem has been noticed by privacy technology researchers at Karlstad University who suggest the use of privacy enhancing technology (PET) in battle contexts [FFH18].
2. The targeting of civillians with misinformation for the purpose of destabilization (A2). The impact of such tactics when applied against massses (A3) has been seen in the manipulation election services deployed by Cambridge Analytica in 2016 [Be18]. Military personnel and their families recently have been exposed to such tactics, for example during NATO exercises in the Baltics where wifes of Dutch military pilots reveived threatening phone calls [6].

Individuals may come under surveillance and may suffer from intelligence actions that steal their identities. Eakin [Ea17] describes in his essay 'The Swedish Kings of Cyberwar' a joint intelligence effort called WINTERLIGHT where intelligence targeted the whole spectrum of identities from access control credentials up to fabrication of 'real' LinkedIn pages in the name of targets. The aforemention propaganda against soldiers' families are part of these tactics. A. Pfitzmann warned against naive application of RFID identification of humans in 2007 through the example of person-specific bombs that explode when certain person's RFID passport walks by [7] (category A2).

A suspected intelligence cyberattack agaainst a Dutch issuer of commercial web certificates, *DigiNotar*, The provider was hacked and then used to issue large numbers of fake domain certificates [vdM13, WB18]. The issued certificates were found to be used by intelligence services to intercept SSL-encrypted web traffic. Only after several months this was discovered, and business terminated by the Dutch government[8]. Meulen [vdM13] concludes:

[3] See video 'Slaughterbots' at https://autonomousweapons.org/slaughterbots/ , accessed 2020-02-21
[4] Bruce Schneier about Future Cyberwar, https://www.schneier.com/blog/archives/2018/08/future_cyberwar.html, accessed 2020-02-21
[5] Interview with Keir Giles on Military,com, https://www.military.com/daily-news/2019/09/03/russian-harassment-nato-personnel-families-next-chapter-information-warfare.html , accessed 2020-02-21.
[6] De Telegraf, Telefoonterreur treft thuisfront: 'Russen' intimideren vrouwen Nederlandse F-16-vliegers, 2019-09-19, https://www.telegraaf.nl/nieuws/838014510/russen-intimideren-vrouwen-nederlandse-f-16-vliegers ,accessed 2020-02-21
[7] Neues Deutschland: Personspezifische Bomben mit RFID-Pass, 25.04.2007, https://www.neues-deutschland.de/artikel/108709.regierung-baut-personenspezifische-bomben.html , accessed 2020-02-21
[8] See full description: https://www.enisa.europa.eu/media/news-items/operation-black-tulip, accessed 03-Apr-2020

The DigiNotar disaster was a painful wake-up call for the world, not just for the Dutch government. They provided the stage on which this disaster could unfold. The breach maintained considerable repercussions for various parties around the globe, especially the affected Gmail users in Iran. (...)it is clear DigiNotar is unfortunately not an isolated incident. In the same year, the media also reported on other attacks against RSA and an affiliate of Comodo, another CA. (...) Other examples include multiple breaches against Verisign, another CA, in 2010, which did not come into the public eye until 2012.

Large-scale IdM infrastructures that process vulnerable populations may lead to genocidal abuse (A3). In spite of historic precedence of the perils of mass identification in the Thrid Reich [Al04, Bl01], modern technology facilitates the mass sorting of populations by applying easily isusable technology such as the mass application of facial biometrics in public areas [Bo17]. Other vulnerable scenarios include digital identities for refugees in UNHCR camps who get registered with biometrics, which may expose them to new classes of risks [Ja15] where conflict moves from the physical into the cyber domain.

3 Attack vectors

The attack vectors through identity management need further attention. IdMs are complex systems combining many parties into the execution of multi-party protocols. End users of all levels of knowledge and relying parties without domain expertise are connected to and trust in certificate authorities, access control systems and document archives. Such systems have vast attack surfaces for intelligence, takeover or disruption. Attack vectors, in general, are:

- Traceable and linkable identifiers;
- Recognizable (unencrypted and identifiable) identity attributes;
- Registration attacks against certificate authorities;
- Directory attacks against directory services;
- Denial of service attacks against parts or all of IdM;
- Identifier, token and credential theft and misuse in replay, imposture or social engineering;

Attacks can get launched directed against IdM technology as well as against procedures and administrative staff. A wide overview over attack vectors against IdM is described by Haber and Rolls in [HR20b]. Tradscending digital risks they illustrate - as observed by Conti et al. [Co10] - the threats to IdM that come through physical information on paper or plastic [HR20a].

The observation of use patterns of IdM tokens has been noted by Paintsil [PF10], in particular accommodating tracking risks. Fritsch and Momen show how tracking of ID attributes

over time enables the collection of identity attributes [FM17, MF20], which constitutes an additional intelligence risk of specific types of IdM with observable tokens or personal information.

3.1 Impact

IdM as an attack vector in cyberwar and cyberphysical war will have serious impact. From the examples discussed above we can expect that IdM will be used in cyber attacks to seek the following purposes:

- Personalized surveillance of individuals of interest;
- Personalized and individual attacks (today drone killings, tomorrow run over by a smart car)
- Attacks on infrastructure (IdM compromized - infrastructure compromized);
- Attacks on documents, archives, authorizations, bank accounts et cetera (trolling and bot networks exploiting real accounts for adversary purposes);
- Identification opens channels for personalized propaganda and manipulation (Cambridge analytica, threats, blackmail and distortion).
- Identity is key to personal data that can get weaponized (compromates, blackmail, disruption, interference).

Facing the vast potential consequences of cybebrattacks, IdM should be both hardened and regulated to mitigate the perils of cyberwar.

3.2 Rules and regulation

IdM in cyber conflict relates to many rules and regulations that vendors of IdM might normally not have in mind when they develop or deploy their technology. Starting from the top level, one's ability to use digital identities and related services in undisrupted ways is anchored in the Universal human rights [As48]. Robinson et al. [Ro18] directly relate cyber conflicts that involve personal digital identity or personal data to three articles of the Universal human rights (pp.7). Article 3 guarantees the right to a safe life, article 12 protects the privacy of the individual, and article 19 guarantees freedom of expression and freedom of information against interference.

Further regulation of cyberwar action can be drawn from the rules of war laid forth in the Geneva convention. Specific requirements are the distinction of civilians from military under attack [Ro17] and the minimization of collateral damage to civilians. However, the concept

of cyber collateral damage [RG16] is ill-defined at this time while the IdM infrastructures are configured and deployed in ways that are close to guaranteeing cyber collateral damage on the civil society.

A closer look at privacy and data protection requirements for secure identity management has been taken by privacy regulators and technology experts in the scope of the FutureID project in [Ha13]. The report formulates strong requirements concerning the secrecy, unlinkability, integrity and control over identifiers. Privacy regulation such as the EU General data protection regulation (GDPR) [9] imposes similar strict data protection and privacy requirements on identity providers.

It may surprise that the EU NIS directive [10] does not focus explicitly on IdM as a critical service in society, given its role and its impact in the functioning of society.

4 Conclusion

Identity management (IdM) is an attractive target for cyber attacks. It enables adversarial surveillance, intelligence gathering, and identity theft. IdM can open channels for direct attacks on individuals as well as on large segments of the population, easily scaling up to the level of a genocide. The attack and disruption of IdM will affect, compromize or destroy critical societal services and critical infrastructures.

IdM should therefore be treated as a critical infrastructure of high relevance for societal security. In consequence, IdM needs to consider its weaknesses, implications and impact when attacked for the aforementioned purposes in cyberwar. Vendors and relying parties need to make sure that citizens will not be endangered through easily traceable or abusable digital identifiers. Identity attributes must be protected with high security assurance. Access to critical services and the integrity of digital archives must be preserved with special attention, which will demand protection measures as well as redundancy.

Effort will have to be spent to ensure that identity and access management providers prevent their directory services from becoming 'kill lists' for adversaries. One particular important question will be: How can we protect digital identities against nonconsensual use by other parties for the purpose of cyberwar? Biometric technology and plain-text identity attributes are two specific high-risk areas of IdM.

International laws and treaties may regulate future cyberwar consequences for IdM, however as of now they do not exist. Therefore should IdM be assessed for cyberwar risks and consequences in multiple perspectives: strategic, national security, national sovereignty, and last but not least focusing on the impact on citizens, in analogy to data protection or privacy impact assessments performed for personal data processing.

[9] Regulation (EU) 2016/679 (General Data Protection Regulation), 2016, https://gdpr-info.eu/ , accessed 2020-02-21
[10] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016

We have to accept that IdM is both a critical infrastructure and an attractive target for cyberwar. Vendors and users of the technology need to be aware of the risks and consequences.

References

[Al04] Aly, Götz; Roth, Karl Heinz; Black, Edwin; Oksiloff, Assenka: The Nazi census: Identification and control in the Third Reich, volume 61. Temple University Press, 2004.

[As48] Assembly, UN General: Universal declaration of human rights. UN General Assembly, 302(2), 1948.

[Be18] Berghel, Hal: Malice domestic: The Cambridge analytica dystopia. Computer, (5):84–89, 2018.

[Bl01] Black, Edwin: IBM and the Holocaust: The strategic alliance between Nazi Germany and America's most powerful corporation. Random House Inc., 2001.

[Bo17] Botsman, Rachel: Big data meets Big Brother as China moves to rate its citizens. Wired UK, 21, 2017.

[Co10] Conti, Gregory; Larkin, Dominic Larkin; Raymond, David; Sobiesk, Edward: The Military's Cultural Disregard for Personal Information. Small Wars Journal, pp. 108–118, 2010.

[Du14] Dunlap, Charles J: The hyper-personalization of war: cyber, big data, and the changing face of conflict. Georgetown Journal of International Affairs, pp. 108–118, 2014.

[Ea17] Eakin, Hugh: The Swedish Kings of Cyberwar. The New York Review of Books, 2017.

[FFH18] Fritsch, Lothar; Fischer-Hübner, Simone: Implications of Privacy & Security Research for the Upcoming Battlefield of Things. Journal of Information Warfare, 17(4):72–87, 2018.

[FM17] Fritsch, Lothar; Momen, Nurul: Derived partial identities generated from app permissions. Proceedings of Open Identity Summit 2017, Lecture Notes in Informatics 277, 2017.

[Fr09] Fritsch, Lothar: Business risks from naive use of RFID in tracking, tracing and logistics. In: 5th European Workshop on RFID Systems and Technologies, RFIDSysTech. VDE, pp. 1–7, 2009.

[Ha13] Hansen, Marit; Jensen, Meiko; Marnau, Ninja; Zwingelberg, Harald; Fritsch, Lothar; Rodriguez, Charles Bastos; Aranda, Nuria Ituarte: FutureID Deliverable D22.3 - Privacy Requirements. Technical report, 2013.

[HG08] Hildebrandt, Mireille; Gutwirth, Serge: Profiling the European citizen. Springer, 2008.

[HR20a] Haber, Morey J.; Rolls, Darran: Identity Attack Vectors. In: Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution. Apress, Berkeley, CA, pp. 107–116, 2020.

[HR20b] Haber, Morey J.; Rolls, Darran: Identity Management Controls in the Cyber Kill Chain. In: Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution. Apress, Berkeley, CA, pp. 117–124, 2020.

[Ja15] Jacobsen, Katja Lindskov: Experimentation in humanitarian locations: UNHCR and biometric registration of Afghan refugees. Security Dialogue, 46(2):144–164, 2015.

[Ka16] Kallberg, Jan: Strategic Cyberwar Theory-A Foundation for Designing Decisive Strategic Cyber Operations. The Cyber Defense Review, 1(1):113–128, 2016.

[MF20] Momen, Nurul; Fritsch, Lothar: App-generated digital identities extracted through Android permission-based data access-a survey of app privacy. SICHERHEIT 2020, 2020.

[MHF19] Momen, Nurul; Hatamian, Majid; Fritsch, Lothar: Did App Privacy Improve After the GDPR? IEEE Security & Privacy, 17(6):10–20, 2019.

[PF10] Paintsil, Ebenezer; Fritsch, Lothar: A taxonomy of privacy and security risks contributing factors. In: IFIP PrimeLife International Summer School on Privacy and Identity Management for Life. Springer, pp. 52–63, 2010.

[RG16] Romanosky, Sasha; Goldman, Zachary: Cyber collateral damage. Procedia Computer Science, 95(2):10–17, 2016.

[Ro17] Rowe, Neil C: Challenges of civilian distinction in cyberwarfare. In: Ethics and Policies for Cyber Operations, pp. 33–48. Springer, 2017.

[Ro18] Robinson, Michael; Jones, Kevin; Janicke, Helge; Maglaras, Leandros: An introduction to cyber peacekeeping. Journal of Network and Computer Applications, 114:70–87, 2018.

[SA11] Sigholm, Johan; Andersson, Dennis: Privacy on the battlefield?: Ethical issues of emerging military ICTs. In: 9th International Conference of Computer Ethics: Philosophical Enquiry (CEPE 2011), May 31st-June 3rd, 2011, Milwaukee, USA. INSEIT, pp. 256–268, 2011.

[vdM13] van der Meulen, Nicole: DigiNotar: Dissecting the First Dutch Digital Disaster. Journal of Strategic Security, 6(2):46–58, 2013.

[WB18] Wolff, J.; Braman, S.: 5 Certificates Gone Rogue: The DigiNotar Compromise and the Internet's Fragile Trust Infrastructure. In: You'll see this message when it is too late: The Legal and Economic Aftermath of Cybersecurity Breaches. pp. 81–100, 2018.