Doxing Political Leaders
The German 'Advent Calendar' Case and the Role of Cybersecurity

Conference on "Global Populisms and their International Diffusion"
March 1-2, 2019, Stanford University

Martin Schallbruch
Visiting Fellow, Hoover Institution, Stanford University
Deputy Director, Digital Society Institute, ESMT Berlin
schallbruch@stanford.edu

Abstract
At the end of 2018, a right-wing young hacker published data on more than 1000 German politicians and celebrities on the Internet in the form of an Advent calendar. The aim of the perpetrator was to expose and discredit said persons. The case triggered a strong legal and political debate about cybersecurity in Germany. The article describes the case and the state of the political debate. Finally, the author argues for legal measures to better protect politicians' accounts due to the threat to democracy posed by such doxing attacks on politicians.

I. The "Advent Calendar" Case

The first news article on January 3, 2019, unveiled a case of doxing in Germany on a scale that was never seen before. Doxing is the Internet-based broadcasting of private information about individuals. In the period between December 1 and December 24, 2018, links were published daily via a hacked Twitter account, through which data stored on various sharehosters could be retrieved. The perpetrator designed the publication in the style of an Advent calendar: every day new information about a person or group was released. On December 1, data about a liberal German comedian, Jan Boehmermann, was released to the public. On December 24, the attack ended with the release of information about the CDU members of parliament, including Chancellor Angela Merkel.

In December 2018, the 24 doors of the Advent calendar were gradually published with the personal data of over 1000 well-known personalities, among them were 993 politicians. Journalists, TV presenters, actors, YouTube stars and

other celebrities were also affected. All parties represented in the German Bundestag were involved with the exception of the right-wing Alliance for Germany (AfD). The type of data published varies greatly. Of the vast majority of those affected, only email addresses, mobile numbers and postal addresses are included in the data collection. However, far more extensive material, for example photo collections, chat logs, documents from cloud storages - both official and private information - became available for about 50 persons. Extensive Facebook correspondence was published about the current leader of the Green Party, Robert Habeck, including the messages with his wife and his children. A liberal comedian, who had won a lawsuit against the chairman of the AfD parliamentary group in the German Bundestag, was forced to find 3GB personal data on the internet.

According to current knowledge, the data came from a relatively small number of hacked emails, cloud and Facebook accounts. For the majority of those affected, little data were publicized because they were sourced from hacked accounts of friends, acquaintances or colleagues. The tweets with the links to the data were at first not discovered due to the small number of followers. However, in January 2019, the hacker started using a hacked Twitter account of a YouTube star with more than 2 million followers to spread the links, which led journalists and security agencies to discover the doxing attack and the "Advent calendar."

Within two days, the Federal Criminal Police Office (BKA) was able to determine the identity of the hacker and arrest him in a small town in Hesse. He was a 20-year-old student who lived with his parents. The court case has not yet begun, but according to all the information published so far, the hacker carried out the action alone, but relied on the technical know-how of other hackers. The suspect, a politically right extremist, was already active in the past in circles of right-wing extremist hacktivists and attracted attention in various forums through posting extremely right-wing and anti-Islamic remarks. According to his own statements, he wanted to demonstrate and discredit the affected politicians and celebrities with his action.

For the persons affected by the data leak, the data dump had very serious consequences. Prominent politicians such as the former chairman of the SPD, Martin Schulz, or the former foreign minister Sigmar Gabriel, received dozens of insulting emails, text messages and calls to their private accounts and telephone numbers. They were forced, like many other MPs, to change phone numbers and email addresses. Green leader Habeck even completely closed his Twitter and Facebook accounts.

II. The Cybersecurity Debate

Although this case involves a relatively small number of data leaked and persons concerned, it has triggered considerable political debate in Germany. Above all, the involvement of almost all leading politicians and prominent journalists has built up enormous pressure to prevent similar cases from happening in the future. Accordingly, the responsible ministers of the federal government and the responsible persons in parliament immediately announced legislative and operational measures to respond to the incident. The Federal Minister of the Interior, Building and Community, announced that he will present a draft "IT Security Act 2.0" by the summer of 2019, which will also include measures for better protection against such doxing attacks.

The debate in Germany on improving cybersecurity to protect individuals against doxing attacks centers around three different starting points: promote better protection of personal data in digital services, demand better and faster reaction to doxing releases, especially from platform operators, as well as assign more far-reaching powers to the security agencies in the fight against doxing. The following is an overview of the various proposals.

(a) Protection of Personal Data

The main reason for the successful hack was the weak protection of user accounts. Access to user accounts on social media, email and cloud services in Germany is still largely protected only by usernames and passwords. Two-factor authentication (2FA) has yet to be fully implemented by the public. In the 2017 Bundestag election campaign, Facebook invited candidates to enable 2FA as added protection to their Facebook accounts. According to Facebook, only 2.1% of the candidates made use of this option. Although Art. 32 of the EU General Data Protection Regulation (GDPR), which came into force in 2018, demands the use of technical security measures to protect accounts, neither the regulation nor the Data Protection Commissioners have clarified whether 2FA is required by law.

At the same time, the operating systems and standard programs used in the consumer sector remain relatively insecure. According to various studies, the number of vulnerabilities in the most widespread software products for consumers has remained stable for years. However, the recent surge in exploitation of such vulnerabilities by malware and the phishing of user IDs have escalated the likelihood of personal data breaches. The increase in the liability of software manufacturers for the security of their products, which has been discussed in Germany for years, has not yet been achieved.

Politicians have therefore proposed to increase the requirements for service providers to protect accounts, for example through mandatory two-

factor authentication. In addition, there is discussion about creating incentives for companies to launch products with strong security features on the market by introducing "IT security labels" for products. This is part of the forthcoming adoption of the EU Cybersecurity Act. It defines a system of voluntary cybersecurity certification in Europe, which could be the basis for the proposed labels.

(b) Platform Responsibility

The distribution of the links to the leaked data sets took place via Twitter. Just a few hours after the links to personal data were made public, Twitter blocked the respective account, so that the 24 "Advent Calendar" tweets and thus the links to the data were no longer available. Access to the data remained possible on the servers of more than 50 different sharehosters worldwide. The perpetrator had stored all data on several services. Together with the Federal Criminal Police Office (BKA), the Federal Office for Information Security (BSI) made an effort to block all these databases. This was successful with domestic service providers or providers within the EU but proved more difficult with international sharehosters. Even after several weeks, the government had not succeeded in blocking all data sets.

Politicians are therefore discussing whether the platforms should be legally obliged to carry out such content blocking within a certain period of time. Reference is made, for example, to the "Netzwerkdurchsetzungsgesetz" (Network Enforcement Act), which imposes a blocking obligation on Facebook, Twitter and others for Hate Speech and other punishable content with short deadlines and steep fines. Furthermore, some politicians are demanding that sharehosters and/or platforms should be obliged to recognize and prevent the upload of leaked data through filters, similar to child pornography or, more recently, certain copyrighted materials.

(c) Tasks and Powers of Security Agencies

Until the first news stories on January 3, no German security agencies had noticed the "Advent calendar" and thus the doxing case. Although the BSI had already been informed about individual’s data leak from members of parliament for weeks, it had not been able to interpret this as related facts. However, neither the BSI nor other security authorities are in charge of detecting leaked information about politicians or other celebrities on the Internet. Also, the protection of accounts of candidates or active politicians does not fall under the legal mandate of the agency. The BSI is only responsible for the protection of the government, monitors in this respect the accounts of the government and also carries out an Internet monitoring for leaked government information.

There is currently a political debate to entrust the BSI with the task of identifying and preventing the appearance of sensitive information of politicians on the Internet in the form of an "early warning system." This requires a change in the law, which could be included in the "IT Security Act 2.0." With regard to legal changes, the increase of the penalty for hacking or receiving and managing stolen data is also being discussed. This is intended to increase deterrence. The current penalty is three years.

Of particular sensitivity and political intensity is the question of the establishment of a power for the security authorities to delete data on servers abroad. So far, for certain, there are very few cases where only the military is allowed to carry out cyber operations abroad. The prerequisite, however, is a corresponding UN, NATO or EU mandate confirmed by the Bundestag. Police hazard prevention or intelligence units may not carry out any active cyber defense. The government's intention to make changes were confirmed by the doxing case and the partly unsatisfactory response of the sharehosters. However, this is a very controversial question in German politics. There is no clear consensus even among the ruling coalition.

III. Theses and Recommendations

1. *The cyber security of digital consumer services is inadequate. By using these services Politicians are taking a serious cybersecurity risk.*

In their private use of digital services, politicians act as consumers. Over the past few years, the market for digital consumer services has been developing very rapidly. It is characterized by high innovation, strong virtualization of offerings and increasingly complicated interconnection of hardware, software and services. At the same time, the cybersecurity of digital consumer services remains inadequate and is improving very slowly. As users of such digital services, politicians, like all citizens, are at great risk of becoming victims of data hacks and leaks.

2. *The extent and depth of personal data that is available through hacked digital services renders any person in public life susceptible to be seriously discredited.*

Especially in a profession as demanding as that of a politician, which embraces many communication relationships, one is dependent on the intensive use of digital services. Without social media, cloud storage, shared calendars and cross-device synchronization, politicians' everyday life can no longer be managed efficiently. At the same time, this strong digitalization gives access to a multitude

of private, professional and political information about individual politicians. Linking such information together or publishing it can seriously discredit the politician. An arbitrary compilation of digital data from various sources can often lead to questions raised about an individual that are unfavorable to him or her in public debates.

3. *The protection of democracy requires protection of politician's and candidate's digital footprints.*

If enemies of democracy succeed in discrediting the top political personnel of the democratic parties, approval for the democratic system and its representatives may decrease, which could in turn promote populism. Protecting democracy therefore also requires protecting the representatives of democracy. Just as personal protection against physical attacks is paramount, protection against digital attacks must also be prioritized.

4. *The approach to Critical Infrastructure Protection is not applicable to the protection of politician's digital presence.*

The discussion on the policy response to the data leak calls for politicians to be treated as "critical infrastructures" for which the European NIS Directive defines cybersecurity measures. The temptation holding politicians accountable for their digital footprints, similar to the approach of responsibility determination in critical infrastructure cybersecurity is not a suitable approach. Critical infrastructures have operators who are held responsible for the cybersecurity of the systems. Such an analogy is feasible for state institutions. However, politicians acting as private individuals are not themselves operators of IT systems. As private individuals, they use the systems of third parties, e.g. platforms like Facebook or iCloud. Politicians would therefore not be able to themselves implement the requirements that apply to critical infrastructure operators.

5. *Providers of basic digital services with strong market positions should be obliged to offer premium-protected accounts, which could be used by politicians.*

One solution could be that commercial providers of cloud, email or social media services could be legally obliged to offer specific accounts with premium protection. These accounts would have to be operated with a higher level of security, integrated with appropriate security measures (e.g. 2FA) and should be subject to special monitoring. The obligation could be limited to market-strong companies to protect small providers. Politicians could oblige themselves by way of a voluntary commitment to use only such accounts. The government should reimburse the extra costs resulting from the use of that kind of services.