Cyber Attacks on Free Elections

Political elections are still conducted using paper ballots. In an age when we use the internet to find information and do our shopping, use apps to control home heating and even use online functions for ID cards, this is quite astounding. Wouldn't it be much easier and more convenient to vote for our politicians from our home computers or smartphones? Our author thinks not – and warns that, even without online elections, many electronic methods threaten to manipulate such processes.

TEXT **RAINER W. GERLING**

To make it clear from the start: there will be no online political elections for the foreseeable future – at least not in Germany. And that's a good thing. Of course, internet voting would be easy and convenient, and it's even possible that more people might vote online. Nevertheless, conducting an entire election process online is an idea that is better left alone. Voters' computers could be attacked from anywhere in the world, and the door would be wide open for various parties to manipulate proceedings. Ronald L. Rivest found an apt way to describe the matter: during a lecture in 2016 he answered a question regarding best practices for an internet election by asking what the best practices were for playing in the middle of a busy street.

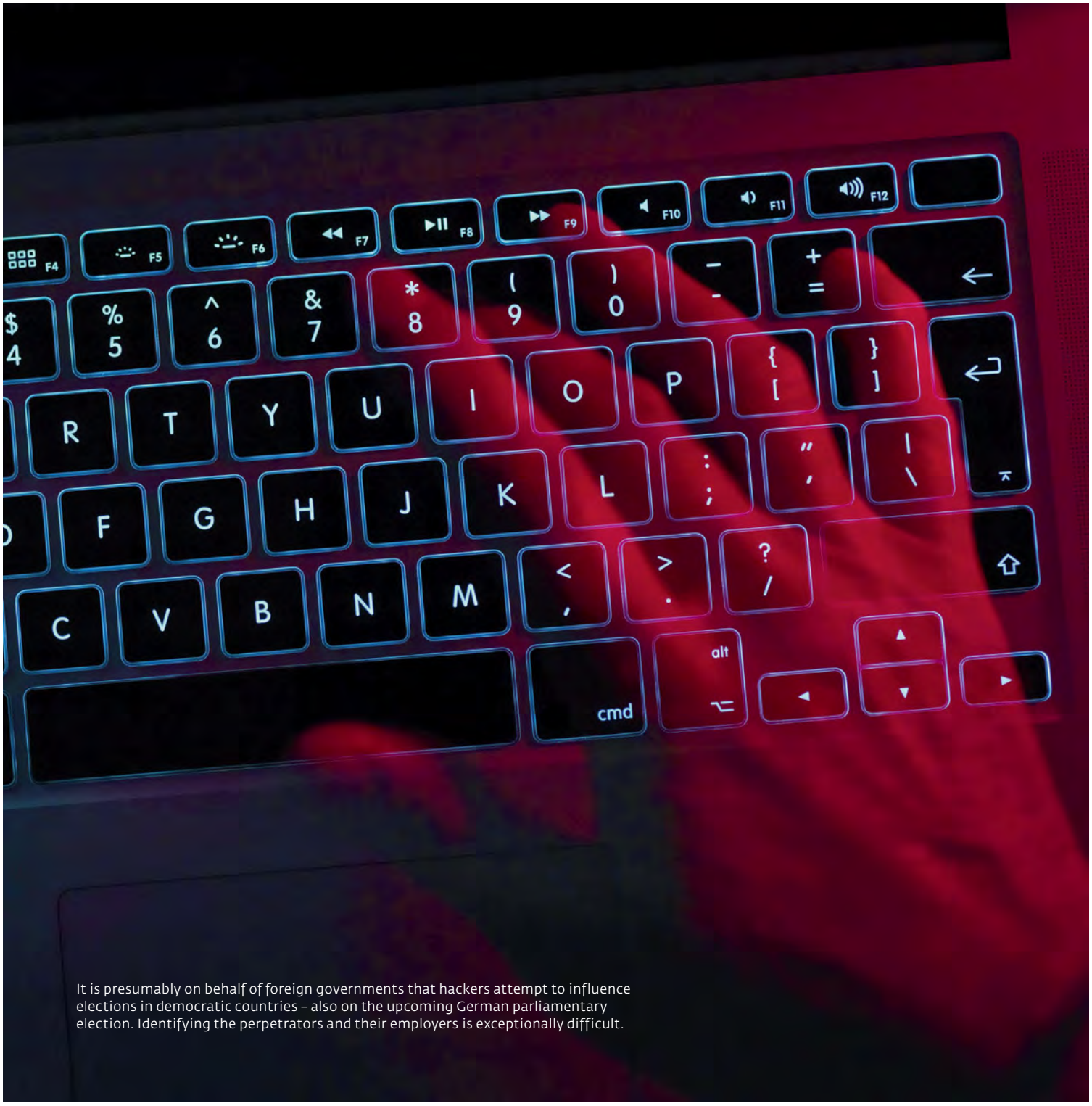
Paper ballots are now used for voting in just 18 US states

Elections must be secret, free and secure. Secret means that nobody finds out how a voter voted. For an election to be truly free, voters must also not have any record of how they voted. Documenting your choice with a mobile phone photo from the voting booth isn't a good idea, either. It must be ensured that votes for a given candidate can't be bought or extorted. Secure means that the votes can be counted without manipulation. It's at this point that a certain degree of doubt surrounds voting machines such as those commonly seen in the US.

In the United States, only 18 of the 50 states still use exclusively paper ballots to cast votes. Ten states use at least some voting machines with no paper printouts (for potential manual recounts). With these devices, checking the digital vote count after the election is virtually impossible. Even when voters receive a paper slip to check their vote, which they then place in a ballot box, ordinary people still can't be certain that the machine recorded the same vote.

In principle, a mistrust of voting machines is advisable: there have been issues in the past with such devices' software. In 2008, it came to light that voting computers produced by Premier Election Solu-

Photo: picture alliance/Cultura R



It is presumably on behalf of foreign governments that hackers attempt to influence elections in democratic countries – also on the upcoming German parliamentary election. Identifying the perpetrators and their employers is exceptionally difficult.

tions "forgot" a portion of the votes when collating results from multiple voting machines. As a new approval process would take years, the company published a workaround in the form of amended operating instructions. This didn't technically prevent the operating error, but merely showed the operator how to avoid the error, so errors aren't precluded.

Voting machines' security systems are also extremely dubious. In a blog post for the Princeton Center for Information Technology Policy entitled *Decertifying the worst voting machine in the US*, expert Jeremy Epstein detailed the unbelievable security gaps in voting computers. For example, the encryption code for the Wi-Fi network's WEP security algorithm is "abcde." This code is "hard wired" and can't be changed. Some systems have gone without security patches since 2004. USB ports and other physical access points aren't always secured. If somebody can insert a USB device into an unsecured USB port, they can probably manipulate the machine. Bruce Schneier, an internationally recognized American IT security expert, reported that voting computers have the default passwords "abcde" or "admin". In addition, since voting computers also communicate via Wi-Fi, they are even susceptible to remote hacking.

Manipulated software teaches voting machines to play chess

In 2007, Dutch and German hackers demonstrated that a Nedap voting machine could be taught to play chess by adjusting its software, showing that the software could be amended as desired without authorization. Hacking voting machines certainly requires a lot of effort, but from the hacker's perspective, the serious implications resulting from a successful hack clearly justify the effort. Moreover, while companies have a strong interest in ensuring that their computer systems are secure and have security systems such as a firewall to protect against attacks from outside, in the case of voting machines, the operator is also a possible attacker. The operator can introduce extensive updates to the machine without arousing suspicion. Voters and election workers are also unable to carry out on-site inspections. Protecting the machine against manipulation by its operator is a much greater challenge.

Completely sealing off voting machines isn't an option, as the ballot papers, at least in their current form, must be programmed before each vote. This is generally done by inserting memory cards, which are often written using Windows computers. The same memory cards also serve to update the software: if a file with a specific name is present, the machine detects the file content as a software update and installs it. Anyone with access to the voting machine for even a short period can insert a memory card and introduce any arbitrary software.

The security of voting machines is rightly considered to be dubious; however, comprehensive manipulation is improbable. If voting computers are hacked, it can be assumed that not all models are affected, but rather only certain ones. Even with normal computers, we know that a hack of a Windows computer won't necessarily work with an Apple or Linux machine. And in the United States, 53 different voting machines produced by 17 different manufacturers are currently in use.

Furthermore, there is no evidence to date that voting computers have actually been manipulated. A group that includes the director of the University of Michigan Center for Computer Security and Society, J. Alex Halderman, alleged that Hillary Clinton received 7 percent fewer votes in Wisconsin constituencies that used voting machines compared with constituencies that used paper ballots. However, these differences could also be explained by systematic errors or random correlations between the type of voting machine and demographic factors. Therefore, we can only speculate as to whether US presidential elections were manipulated, but an unpleasant aftertaste and an uneasy feeling remain.

Voting machines have also been used in the past in Germany in various elections. Following two complaints against "the use of computerized voting machines," the German Federal Constitutional Court in 2009 declared the Federal Voting Machine Ordinance

to be unconstitutional "because it does not ensure the approval and use of only such voting machines as satisfy the constitutional prerequisites of the principle of publicity." One prerequisite is "that the main steps in the election process and the calculation of results can be inspected by citizens reliably and without the need for specialist knowledge." Current voting computers do not guarantee this. As a result, voting computers haven't been used in Germany since that time.

The question remains as to which factors speak in favor of the machines, if any at all. The only advantage is that they make counting simpler, faster and cheaper. They don't make the voting process easier for voters. Voting machines merely prevent invalid ballot papers from being submitted – but submitting an invalid vote can also be a conscious voting decision.

There are also many good reasons to retain classic paper ballots in political elections. Only when we are able to mark a ballot with a normal pen on normal paper can we ensure that counting takes place promptly and publicly – observing the principle of multiple-assessor verification. This verification principle is also ensured by having observers present when votes are cast.

Nevertheless, voting machines have probably not been banished from German polling stations for good. Manufacturers and local authorities with an eye on their funds will again attempt to introduce electronic systems to cast and tally votes. If voting machines are introduced, it mustn't be done by reasoning, "trust us, we'll do it right." And that "we" could be both the voting machine manufacturer and the state. The fundamental approach must be: "Glitches will occur, we have to identify and correct them." The possibility to conduct an audit must be included as part of an electronic voting process, and an audit of the election results absolutely must be carried out.

In the German federal elections in 2017, there will be no manipulated voting machines, but by no means does this preclude the risk of digital manipulation: voting results must be collected from polling stations, which is done over digital networks. Dieter Sarreither, the Federal Returning Officer, expects cyber attacks and has therefore had the administrative network well secured as a precaution. If necessary, telephone and fax communication can be used instead. In the election in the Netherlands on March 15, 2017, votes were counted by hand, as the software used to do so is considered to be susceptible to hacking. Couriers brought the results from the polling stations to regional election offices. Only then were computers used.

In Germany, the elections themselves can thus certainly be considered secure, but there is cause for concern that hackers may attempt to influence the

Digital criminals leave behind traces, but concrete evidence is rare

result during the run-up. This was clearly the case in the US: on January 6, 2017, the CIA, FBI and NSA published a joint report stating that Russian intelligence services had influenced the US presidential election. In addition, the computer network of the Democratic National Committee was hacked in July 2015. Large-scale document theft occurred through May 2016. These documents were later published by DC Leaks and WikiLeaks under the (potentially Russian) pseudonym Guccifer 2.0. As these documents were primarily intended to discredit the Democrats and their candidate, Hillary Clinton, this can be regarded as influencing the election – or at least attempting to do so. The Russian government has adamantly denied involvement.

There is no publicly available evidence that Russian intelligence services were behind these events. There are, however, fairly strong indications. Of course, such indications of digital wrongdoing are not as easy to identify as real-world evidence: at a classic crime scene, police find fingerprints, fibers and DNA traces that they can ultimately attribute to one or more individuals. With a digital crime scene, investigators find malicious software and IP or e-mail addresses when analyzing communications,

Photo: picture alliance/Cultura R

but attributing these bits and bytes to an individual is much more difficult than is the case with conventional evidence.

So digital forensic experts look, for example, for Russian or Chinese text fragments in the malware. This alone isn't proof, as it's entirely possible that a hacker from another country might have laid a false trail. If the forensic expert is lucky, the malware might be an optimized or advanced version of known malware that Russian or Chinese state services are known to have used in the past. There are then two clues. Data captured in a hack is transmitted to a server. This server is located with a provider somewhere in Europe or America. For this, the attackers simply rent computers from service providers and register domains. However, if the domain name was registered using an e-mail address that has previously been linked to Russian or Chinese state services, then this constitutes a further piece of evidence. The specific data transmission technique used might already be known to the investigators, and they can compare it with previous cases. The precise technical details of this analysis, however, are a closely guarded trade secret of the investigating secret services.

The interests involved may be a further clue: there is a high probability that an attack on the World Uyghur Congress would involve Chinese state agencies, as the World Uyghur Congress is one of the Five Poisons, the main threats to the Chinese state. If, however – as occurred on December 23, 2016 – a large power outage causes problems in Western Ukraine, and can be traced back to a cyber attack, then it is highly unlikely that Chinese state services are behind it. Several aspects here point toward Russian origins.

Extensive knowledge collected by security firms and authorities may be able to produce a plausible overall picture. The conclusive findings are published, though they aren't easily comprehensible from the outside. And of course a plausible picture is certainly not evidence that will stand up in court. In light of the events surrounding the US presidential election, the question is whether the German federal election is similarly vulnerable. At any rate, there have already been multiple cyber attacks on German political parties and governmental structures in the past 24 months.

In early 2015, hackers broke into the Parlakom network of the German Bundestag and copied 16 gigabytes of data. German security services believe that a hacker group close to the Russian state, known as APT28, among other names, was responsible for the attack. This group has been active since around 2004.

Attackers might attempt to manipulate public opinion before the German federal elections

The attack on French television broadcaster TV5 Monde in April 2015 was also attributed to APT28, as Hans-Georg Maaßen, President of Germany's domestic security agency, the BfV, described in a podium discussion at the Max Planck Society's IT Security Symposium in 2015. The attacks also served as a false flag operation, as the hack included a presumably faked claim of responsibility from a previously unknown Islamic group named Cyber Caliphate.

IT security company Trend Micro reported in May 2016 that the APT28 group had launched an attack against the CDU. It was done by operating a replicated CDU webmail server in Lithuania in order to tap user accounts and passwords through phishing e-mails.

In August 2016, one Heinrich Krammer sent an e-mail that seemingly came from NATO headquarters (the e-mail address ended in @hq.nato.int). The e-mail promised background information about, among other things, the military coup in Turkey. Anyone who clicked on the link installed malicious software on their computer. The e-mail's addressees were Sahra Wagenknecht and the head office of the political party *Die Linke*, as well as the CDU and its youth movement, *Junge Union*, in the Saarland. APT28 is suspected in security circles to have been behind this attack, too.

In November 2016, WikiLeaks published 90 gigabytes of data (2,420 documents) from the German Bundestag's commission investigating the NSA affair. This data didn't appear to originate from the

Photo: picture alliance/Cultura R

Bundestag hack in early 2015. The parallels with the hackers' approach in the US are obvious. Consequently, it must be expected that, when the election campaign in Germany heats up, information from these hacks will surface on WikiLeaks or similar platforms.

The Federal Office for Information Security (BSI), Germany's national cyber security agency, is working intensively on the issue. In autumn 2016, BSI President Arne Schönbohm personally warned German political parties about reconnaissance conducted by hackers affiliated with other states. The suspicion is that attackers might attempt to manipulate public opinion prior to the German parliamentary elections. The focus is on opinions and ideas being posted on the internet or social networks by automated means. In March 2017, the BSI again expressly warned German political parties of expected cyber attacks during the election campaign.

In early February 2017, media reports stated that German secret services had found no evidence of targeted Russian disinformation. However, according to research by broadcasting companies NDR and WDR and the Süddeutsche Zeitung, the 50-page report described the reporting of Russian propaganda media such as the German-language versions of Russia Today and Sputnik News as downright "hostile." Where is the line between exaggerated reporting and disinformation?

States attempting to influence public opinion to suit their aims through disinformation, propaganda, fake news and alternative facts (once known as lies) is nothing new. However, as a result of the internet, social media and platforms such as WikiLeaks, the number of information providers has dramatically increased, and traditional journalistic ethics and truthfulness are often left by the wayside. It's difficult for traditional media and experts, or even state agencies, to make corrections and evaluations. Experience tells us, however, that if you throw enough mud, some is sure to stick. Ultimately, each citizen must decide for themselves what they believe and what they don't. Only one thing can help here: education. In that respect, Europeans should be less susceptible to alternative facts than citizens in the US, as the average level of education in Europe is higher. ◀

Photo: Axel Griesch

THE AUTHOR

Rainer W. Gerling, born in 1954, is the IT Security Officer of the Max Planck Society and honorary Professor of IT Security in the Department of Computer Science and Mathematics at the Munich University of Applied Sciences, where he is responsible for additional training on operational data protection. Gerling has published numerous essays in scholarly journals and books, and belongs to the editorial board of the magazines Datenschutz und Datensicherheit (Data Protection and Data Security) and IT-SICHERHEIT (IT Security). Since 2012, he has been Deputy Chairman of the German Association for Data Protection and Data Security (GDD).