Global Challenges
Election Disinformation

INNOVATIONS FOR
SUCCESSFUL SOCIETIES

SWEDEN DEFENDS ITS ELECTIONS AGAINST DISINFORMATION, 2016–2018

Gordon LaForge drafted this case study based on interviews conducted in October and November 2020. *Case published December 2020. The Princeton University Liechtenstein Institute for Self-Determination supported the development of this case study.*

SYNOPSIS

The Russian state information influence attack against the 2016 US presidential election rattled authorities in Sweden. The Scandinavian country of 10 million was already a frequent target of Kremlin-sponsored disinformation. With a general election approaching in September 2018 and public apprehension about a possible influence attack high, officials at the Swedish Civil Contingencies Agency began preparing measures to defend the credibility of the country's electoral process. Rather than attempt to halt the creation and spread of disinformation, the agency aimed to build the resilience of institutions and society overall to withstand information influence activities. The agency trained thousands of civil servants, built and strengthened interagency coordination structures, coordinated with traditional and social media, raised public awareness, and monitored the digital information landscape. Despite a cyberattack on the Swedish Election Authority website that fanned claims of fraud and generated a flood of homegrown political disinformation, the election ran smoothly and the government doubled down on the resilience-building approach for protecting the 2022 election.

ISS is program of Princeton University's School of Public and International Affairs: successfulsocieties.princeton.edu. ISS invites readers to share feedback and information on how these cases are being used: iss@princeton.edu.

INTRODUCTION

Shortly after the US presidential election in November 2016, senior US intelligence officials made certain disclosures that shook authorities in Sweden. The US intelligence community announced it had determined that for several months preceding the vote—and on the direct order of President Vladimir Putin—Russian agents had been carrying out an information influence campaign that was seeking to "undermine public faith in the U.S. democratic process" and damage Hillary Clinton, the Democratic Party candidate in the race.[1]

At the center of the campaign was a massive disinformation operation waged on social media. A Kremlin-linked troll farm called the Internet Research Agency created thousands of social media accounts that purported to belong to Americans, that spread radical content and fake news stories, and that organized physical demonstrations. Researchers found that posts on Facebook from just 6 of the 470 known Russian-created accounts appeared in other users' news feeds 340 million times and were engaged with 19.1 million times.[2] And Facebook was only one of several social media platforms the aggressors used.

Mikael Tofvesson, head of global monitoring and analysis at the Swedish Civil Contingencies Agency (*Myndigheten för samhällsskydd och beredskap*, or MSB), realized there was nothing to prevent a similar attack on his own country's general election in September 2018. Officially neutral but an increasingly close partner with NATO, Sweden had been a regular target of Kremlin-sponsored disinformation since 2014, when Russia annexed Crimea and ramped up its use of influence operations across Europe. Social media accounts, bot networks, and Russian state-TV outlets in Sweden created and spread fake news and forged government documents to sow dissent about national security policy and inflame division around the issue of migration, which had been a societal flashpoint since 2015, when Sweden's center-left government accepted 163,000 asylum seekers fleeing war in the Middle East.

Widespread use of social media and a proliferation of online alternative news and opinion sites meant disinformation spread more easily: nearly 97% of the Swedish population had internet access, and in surveys, 86% of Swedes said they obtained news online, including 51% from social media.[3]

The MSB was in charge of coordinating the management of crises and emergencies, such as wildfires, chemical spills, and bomb threats. Tofvesson, a former intelligence official, was hired at the MSB's inception in 2009 to create the global monitoring unit, which was responsible for identifying emergent issues that threatened public safety, national values, and the functioning of society. Foreign information influence was one such issue.

A Swedish election had never suffered a major disruption, and turnout in the 2014 vote was 85.8%—among the highest rates in the democratic world—yet with revelations from the United States fueling media interest, public concern, and high-level political attention, Tofvesson prepared an internal task memo explaining why the coordination of a defense of the 2018 Swedish election against a foreign-influence campaign was a job for the MSB.

The director general approved, granting Tofvesson the authority to move ahead with the project.

THE CHALLENGE

The primary challenge for Tofvesson and the MSB was that there was no legal basis for stopping the creation and dissemination of disinformation. Freedom of speech, even deliberately false speech, was protected by law. "The democratic issue here is that it's OK to be wrong, and it's not up to the government to say if someone is lying," Tofvesson said. "You have the right to freedom of speech and to anonymity in that speech." Moreover, both domestic entities and foreign entities could establish and operate media outlets in Sweden, purchase advertising, and even make campaign contributions to political parties.

A second challenge was that the structure and culture of Sweden's administrative state made interagency coordination difficult. Identifying, containing, and countering disinformation required communication and collaboration between the government agencies involved in elections, yet those agencies were highly autonomous and independent. They had credibility and power, but they were also siloed and not predisposed to collaboration (text box 1).

The biggest disconnect lay between the election authorities and the agencies responsible for securing the election: mainly the Swedish Police Authority, which was responsible for law enforcement and public safety within the country, and the Swedish Security Service, which was the separate counterterrorism and counterespionage agency. With the exception of some high-level contact between the national Election Authority and the Swedish Security Service, these two worlds did not plan, coordinate, or otherwise interact with one another. An

Text Box 1: The Swedish Government

The Swedish government was a parliamentary democracy in which the parliament enacted laws and appointed a government headed by a prime minister, who in turn appointed 22 cabinet ministers. The ministries recommended policy to the government, but the implementation of policy fell to 345 highly independent government agencies staffed by civil servants. Though overseen by the ministries, the agencies had power, personnel, and money. They enjoyed a high degree of autonomy and a reputation for being apolitical. Individual cabinet ministers had no power to instruct an agency. The cabinet as a whole could issue government orders to the agencies so long as the orders did not concern a particular person, company, or case—a safeguard against corruption—but it seldom used that power.

At the subnational level, Sweden was divided into 21 counties, each managed by a county administrative board. Each county contained several independent municipalities that, among other things, collected taxes, administered education and many social welfare programs, and conducted elections. There were 290 municipalities in total, and they varied widely in population and resources. As of 2017, Stockholm, the capital city, had nearly 1 million people; Bjurholm in the far north had 2,442.

incident in the 2014 general election illustrated the problem: A gang of neo-Nazis had intimated voters and had damaged materials at a polling site in Stockholm. But by the time the police arrived, the gang had moved on and shortly thereafter attacked another polling site, which was unprepared because the police hadn't warned other polling sites or communicated the threat to election authorities.

The lack of coordination was especially problematic at the local level. Elections were conducted by Sweden's 290 municipalities, which varied widely in size, resources, and capability. Each was responsible for administering and securing the vote, but in many cases, a municipality's election administrators, poll workers, police officers, local media, and postal workers failed to communicate or coordinate with one another. "Disinformation relies on exploiting gaps between different entities," said Edwin Sönnergren, a risk management consultant who worked with election authorities. "If local media aren't talking to the municipality, then it's easier for an aggressor to seed disinformation in one group or the other."

Another challenge was that disinformation could be difficult to identify, as were the threats it posed (text box 2). In the 2016 US presidential election, the disinformation was both voluminous and varied. It took the forms of social media posts, fake news stories, advertising, phony data, and doctored images. And throughout the campaign season, US officials, political parties, media, and the public were largely unaware of the threat—in part because no agency was monitoring and analyzing social media. It wasn't until *after* the voting that the intelligence agencies affirmed the existence of a foreign operation that had

Text Box 2: Disinformation

The MSB had a mandate to counter influence operations against Sweden, which it defined as activities carried out by a foreign power to affect the perceptions, behaviors, and decision making of target audiences in Sweden. In its election defense project, the agency focused on countering disinformation about the electoral process. Though disinformation threats often occurred in cyberspace, they were not considered cybersecurity threats, such as hacks of voting systems or thefts and disclosures of the e-mails of political candidates. Cybersecurity was the purview of security and intelligence agencies.

Disinformation was deployed through traditional and social media. Types of disinformation included fake news, false statistics, phony experts, fabricated government documents, manipulated images and video, and information that was deliberately misleading, deceptive, or provocative. Disinformation was spread and amplified through bots (software or humans that exhibited automated online behavior), troll farms, and fake accounts and fake groups on social media. In a typical process of disinformation, an aggressor would identify a target audience, create fake groups on social media, spread specious news and information using those groups aimed at the target audience, amplify that information by using bots, and even engage the target audience in the physical world by organizing demonstrations.

sought to undermine the election and denigrate one of the presidential candidates.

Finally, the risk of disinformation was amplified by the unusual nature of voting in Sweden—a process that required the national Election Authority in 2018 to print 673 million ballot papers for an electorate of 8 million. Each of the country's 290 municipalities was responsible for conducting elections and performing a preliminary vote count. County administrative boards performed a second, official count. The national Election Authority's role was to procure and distribute election materials, register political parties, issue guidelines, inform the public about where and how to vote, set the boundaries of municipal voting districts, and certify the final results. The authority, which had a permanent staff of only 22, was supported by the Swedish Tax Agency, which provided population information for voter rolls and supplied logistical, technical, and personnel assistance.

Every four years, on the second Sunday of September, Swedes went to the polls to vote in three separate elections: municipal, county, and national. Registration was automatic. Swedish citizens at least 18 years old had the right to vote, and non-Swedish permanent residents could vote in municipal and county elections but not national ones. During an early voting period, which began 18 days before each election day, voters could cast their ballots at any of nearly 3,000 polling sites, located in such varied places as libraries, municipal buildings, subway stations, and even Ikea retail stores. On election day, voters could cast a ballot at an early voting site, or at their designated polling site in their home municipality, where they also had the option to change their vote if they had voted early.

Although the system was decentralized, manual, and transparent, Sweden's unusual approach to handling and distributing paper ballots left the door open to allegations of mismanagement and malfeasance. Each political party had its own ballot paper that listed a party's slate of candidates, and party members passed them out freely to voters during the campaign. Some parties had multiple ballot papers with a different slate of that party's candidates on each ballot paper. All parties' ballot papers were displayed in racks at polling sites, and voters had to select and cast one for each of the three elections (national parliament, county, and municipal). In the 2018 elections, 79 parties ran in the parliamentary election, and about 20 or 30 parties ran in each county and municipality.

The system had its roots in a cultural tradition whereby candidates would visit towns and hand out their parties' ballot papers for voters to take home and study, but reports of lost, discarded, or stolen ballot papers led to claims of fraud. And even though ballots cast at the polls by registered voters were the only ones that got counted, problems and disputes arose when ballots for specific parties ran short or disappeared for no apparent reason, possibly leaving poll workers with insufficient supplies. Plus, supporters of a party might claim fraud or bias if their parties' ballots were missing or taken.

Petter Nyhlin, an MSB official involved in interagency coordination, recalled, "When I learned how extremely complex and logistically difficult the system was, I was humbled: there were so many opportunities for mistakes, and I knew trolls could amplify and exaggerate any mistake."

FRAMING A RESPONSE

In early 2017, the MSB launched its project to support defense of the 2018 election. Tofvesson assigned management of the preparations phase to Sebastian Bay, a member of the MSB Counter Influence Unit who had a background in countering foreign influence operations in the Swedish Armed Forces.

The MSB strategy would focus not on stopping the influx of disinformation but, rather, on equipping Sweden's population and institutions to withstand it. As an open, democratic society that valued freedom of expression, the authorities were not permitted to stanch the spread of falsehoods. So, instead of taking a top-down, regulatory approach, the MSB aimed to bolster societal resilience from the bottom up.

Sweden had a long tradition of resilience. Officially neutral in both World War II and the Cold War, the country's national security doctrine prioritized civil or so-called "total defense," whereby every citizen prepared for war or crisis. Since the early 1950s, an explicit component of that doctrine was "psychological defense," which consisted of education, training, and exercises to help Swedes identify and resist propaganda and information warfare.

The MSB was the torchbearer of that tradition. It was created in 2009 from a merger of the Cold War–era Board of Psychological Defense and the Rescue Services Agency and Emergency Management Agency. The MSB's modus operandi was to strengthen systems in order to prevent worst-case scenarios from occurring in the first place. "The basis of the MSB is fire protection," said Bay. "The MSB doesn't try to predict who might start a fire, and it doesn't usually put fires out. It issues guidelines and advice, such as where to put fire alarms and how to work in a systemic way to prevent fires."

The MSB's main jobs were crisis coordination and support. Sweden had no umbrella crisis management agency. Rather, each government agency was responsible for handling emergency incidents within its individual area of responsibility. The MSB supported those agencies with knowledge, funding, equipment, and coordination structures. Yet with few exceptions—such as requiring incident reporting and issuing public safety guidelines for topics like fire protection—the MSB had no authority to compel any other agency to do anything beyond providing information.

When it came to countering information influence, the MSB's mandate was restricted to dealing with threats posed by foreign interests. "We don't touch internal disinformation actors, even if they're extremists," said Tofvesson. "The MSB is technically a national defense capability, and we don't use defense capabilities against our own population."

Other agencies, however, including the election authorities, did have mandates to counter homegrown disinformation targeting their areas of

responsibility, and the MSB provided them with knowledge, training, and other support to help them counter disinformation activities. "All the things we would do to strengthen resilience and better prepare our systems against foreign operations would, of course, help guard the system against domestic actors," said Bay.

In framing a defense of the electoral system against any influence campaign, Tofvesson and Bay took a first step by painting a situational picture to determine the Swedish election system's vulnerabilities. They studied Russia's attack on the US election, and they interfaced with foreign counterparts from the United States, the United Kingdom, and various European countries to learn how other democracies were assessing and addressing the threat.

The MSB invited the Swedish Election Authority to deliver a briefing on how elections worked. The MSB team met with a few municipal and county election authorities in and around Stockholm and sent out a questionnaire to all 21 county administrative boards, asking them to report on how they assessed threats of information influence activities, how they prepared for them, what their own vulnerabilities were, and what they needed. In addition, the Security Service conducted a classified threat assessment that it shared with the MSB and other agencies.

What Bay and his colleagues quickly learned was that although many officials in Sweden and abroad were fretting about electoral disinformation, there existed very few best practices for handling it, and methods and efforts to prepare for it were nascent. "Sweden had virtually no coordination on the issue of election disinformation and influence operations because no one had really thought about threats of any sort to elections before, much less disinformation," said Bay. Coordinated defense of an election was a new idea. Historically, not even the Swedish Police Authority—whose election operation traditionally focused on managing civil unrest during campaign seasons and usually ended the day before voting closed—was prepared with a uniform national strategy or operation focused on the administration of elections.

From its analysis, the MSB team determined that the threat was not to the electoral process itself. Sweden's elections were manual, decentralized, and transparent—highly robust against failure or attack. And the law contained provisions that allowed for recounts and reruns in cases in which a mistake could have affected the final outcome. The system appeared to be secure. "But what *is* a fact and what can be perceived as a fact are two very different things," said Tofvesson. As Bay put it: "What concerns me is not whether there was a problem with the election; there are systems and laws in place to handle problems. What we can't handle is people *thinking* there has been a problem, when there hasn't been a problem."

Thus, the threat of disinformation was not to an election itself but to public *trust* in the election. Tofvesson determined that damage to trust in an election was ultimately about weakening the credibility not only of the incoming leadership but also of the entire government. "Our ultimate goal therefore was to protect the next government's ability to lead Sweden internationally," he said.

"We were protecting trust not only in the election process but also in the government itself."

Tofvesson and his colleagues further reasoned that based on the US attack, any influence operation against the Swedish election would have four core aims.

1. To undermine trust in the electoral process, such as by spreading disinformation about the reliability and integrity of the election
2. To influence the will and the ability of voters to participate in the election, such as by raising doubts about the credibility of voting procedures, thereby undermining the will to vote
3. To shape voters' political preferences, such as by creating and amplifying fake news about candidates or by hacking and leaking stolen political information
4. To influence and subvert political candidates and government institutions

Those four pillars formed the framework the MSB would use to guide its analysis of the threat and the goals of the different areas of work it pursued. The fourth fell under the mandate of the Swedish Security Service, which handled espionage and cyberattacks. The third was also outside the MSB's mandate because it dealt with the domestic political landscape and not the electoral process itself, though the agency determined it could contribute indirectly by raising awareness, funding researchers, and supporting journalists.

Broadly, the MSB strategy for bolstering the resilience of voters in the election would focus on reducing vulnerabilities and augmenting the system's capacity to counter disinformation. Specifically, that meant raising awareness about the threat, facilitating information sharing among relevant stakeholders, identifying disinformation and influence activities, and enabling coordination between agencies and authorities.

In March 2017, the prime minister published an Op-Ed in *Dagens Nyheter*, Sweden's most-read daily newspaper, assuring the public the government and its agencies would safeguard the election—scheduled for a year and a half later, on September 9, 2018—from any influence campaign. "That helped us in the sense that we had political support for what we were doing—meaning that when we started talking to other agencies about the election, they didn't think it was strange or put up any resistance," said Bay.

GETTING DOWN TO WORK

The MSB's election defense project proceeded in two phases. The preparation phase, which Tofvesson assigned Bay to lead in January 2017, lasted for roughly a year. On his own at first, then joined by a small team later in the year, Bay focused on raising awareness; developing training and guidance for civil servants; establishing and reinforcing coordination; and commissioning research. The team relied on consultants, academics, and media for much of that work.

The second phase began in February 2018, when Tofvesson requested and received approval from the MSB Operations Directorate to turn the election defense project into an official operation. That gave Tofvesson the authority to enlist roughly 30 MSB personnel to work on a task force that would carry on and expand the work Bay had begun during the preparations phase. The task force would provide operational capability for coordinating a crisis response should an attack—information or otherwise—against the election occur. The task force remained operational until a new government was formed in January 2019.

Supporting election authorities

The MSB first focused on providing election authorities with the knowledge, training, and tools needed to understand the threat of disinformation, vulnerabilities in the electoral system, and methods for responding.

In mid-2017, more than a year before the 2018 election, the Swedish Association of Local Authorities and Regions—a local government employers and advocacy organization—in cooperation with the Election Authority began to hold preparatory training sessions for all county and municipal election authorities on new laws and procedures for the vote. Bay was invited to deliver a briefing and answer questions at each training session.

That fall, the training was held 13 times to reach all of the municipal election authorities, plus one for the election authorities at county administrative boards. The MSB team attended each session and gave 90-minute presentations. Their briefings covered disinformation threats, including examples from Sweden and the United States; explained the MSB's approach and rationale for protecting the election; and gave general advice on countering the threats. The material covered only information influence and disinformation targeting the *electoral* process—when, where, and how to vote—not the *political* process.

Municipal election authorities were receptive. Worries about the issue were extensive. In the first half of 2017, stories about Russian interference in the US election had flooded Swedish media. Authorities in many municipalities—especially smaller ones—were aware of the issue but felt ill prepared to deal with it.

Although the briefings succeeded in raising awareness, subsequent question-and-answer sessions made it clear that the municipalities needed more guidance on a topic that was difficult to get a grip on. Most disinformation was ambiguous, amorphous, and often in a gray area between truth and outright falsehood. Among the municipalities' questions were, How can you determine whether something was fake or simply misleading? And then, How *exactly* should you respond? What should you communicate to the public if a piece of fake news, a fabricated press release, or an erroneous report surfaced about the election in your town? Should you rebut it? Ignore it? They were the same kinds of questions that often came back in surveys the MSB had sent out to county administrative boards at the start of the project. Even though Bay was well

versed in the area of counterinfluence, he recalled that he was at a loss: "'What do we do?' they asked. And I said, 'That's a great question…'"

A handbook for communicators

For answers, Bay turned to Professor James Pamment. One of Sweden's leading thinkers in the study of how governments use public communications to influence one another, Pamment headed Lund University's Department of Strategic Communication, where much of his work was in training civil servants involved in public-sector communications, a large and well-developed field in Sweden. One of the responsibilities of municipal administrations was public communications.

Bay invited Pamment to Stockholm and asked him what it would take to equip Sweden's municipalities to counter disinformation. Pamment recalled telling him: "What we need is one hour with every public-sector communications officer in every municipality in the country. I could develop a training program that would give them the basics of what to look out for and would empower them to make sensible decisions about what to do." Two weeks later, Bay called him back and said he could get him that hour.

Pamment returned to Stockholm and in meetings with Bay and Tofvesson laid out a plan to create a training program on ways public communicators could counter disinformation. The first step would be to write a report detailing the leading scientific thinking and research from the field of strategic communications. That would form the intellectual foundation for a practical handbook and training program. "It had to be anchored in research," said Pamment. "You could ask anyone from a PR company to write you a handbook on how to counter disinformation—and they'd do it—but we wanted something based on research. Even though communications is a soft science, there are clear, established best practices."

Pamment signed a contract with the MSB, and for six months, he and a team of three researchers from Lund University pored over scientific research to develop the report, titled *Countering Hostile Influence: The State of the Art*. The document was 120 pages long and included a diagnostic framework for identifying information influence activities, approaches for countering them, and a chain-of-events model of how disinformation spreads in and affects a society.[4] "'That last piece was a huge step forward," said Pamment. "'There weren't many good explanations for how disinformation affects the media environment and the information environment. The existing models are either military based or overly simplified. We developed this explanation and tested it out and found that people went from having zero knowledge of how disinformation works to saying, 'Oh, I get it. I understand what's happening here'" (text box 3).

Pamment and his team distilled insights from the report into a practical, 50-page handbook organized into three sections: (1) Becoming aware of information influence, (2) Identifying information influence, and (3) Countering information influence.[5] They wrote the handbook with a specific target reader in mind—a small-town municipal administrator in charge of communications.

Text Box 3: Modeling Disinformation and Countering Hostile Influence

James Pamment and his team from Lund University drew from the latest research in communications, sociology, and other social sciences to develop models of ways disinformation affected a society, ways of identifying information-influence activities, and ways of responding to them. For the first model, the researchers described the epistemic chain by which people form opinions in a free society. "Western society is built on free opinion formation in the public sphere," they wrote. Opinions emerged in a person from the interplay of seven systems: the individual, the social sphere, the public sphere, media and forms of culture, elites and officials, experts and expert sources, and science or similar evidence-based systems such as independent journalism. Free opinion formation—and thus the functioning of liberal, democratic society—depended on ideas based on evidence or substantiated claims to successfully compete in the public sphere.

Disinformation exploited vulnerabilities in public opinion (fake experts, unsubstantiated claims), in the media system (new platforms and media that make real news harder to distinguish), and in cognition (biases, heuristics) to undermine free opinion formation.

"You work for a small municipality that has a few thousand people in the north of Sweden, and weird posts start coming up on the town's Facebook feed," said Pamment. "Your full-time work involves writing messages and monitoring what people are saying, but this is a situation you don't completely understand, so there's some uncertainty about what to do. And one of the last things you would think is that this was part of some global campaign led by a foreign intelligence agency to undermine democracy."

The ultimate purpose of communications that identified and corrected disinformation was not so much persuasion but, rather, assurance, Pamment stressed. "It's in large part about assuring the older generation—people who might not fully understand the modern media and technology environments and might worry if they see fake or misleading news on Facebook," he said. "We're not going to change the minds of people who believe fake news. It's about winning the sensible users, the middle ground. And if you provide those people with the facts, then maybe that would help them persuade family members with more-extreme views."

The team traveled across the country, delivering to municipal communications staffs the training that was based on the handbook. The training sessions varied in attendance and duration. Some lasted just an hour—as Pamment had requested from Bay when he first accepted the assignment—but some others were a half day long and included scenario-based exercises.

Pamment also went abroad. He shared the handbook and, along with MSB staff, led training sessions for a dozen government counterparts in Europe and the United States. Several countries—including Finland, Estonia, and Latvia—copied the handbook, revising and translating it to suit their own contexts. Many considered the handbook to be the gold standard in the field.

Protecting elections

In addition to the initial training and the communications guidance, the MSB worked with a team of consultants to develop election-protection best-practice guidelines that could form the basis of a training package for municipal election authorities. The MSB tapped 4C Strategies, a risk management consultancy that had conducted a risk and vulnerability analysis for the election authority of Stockholm ahead of the 2014 election.

The MSB, the Swedish Election Authority, and the Västra Götaland county administrative board, seated in Göteborg, Sweden's second-largest city, contracted 4C Strategies to develop best practices for protecting the election not just from disinformation but also from a host of other risks, such as violence against election workers, sabotage, and personnel and infrastructure failures. "That was new. Traditionally, we had not protected elections in Sweden this comprehensively," said Bay. Making an election more secure and less error prone was critical for mitigating the threat of disinformation. "By ensuring the integrity and smooth functioning of the election, you reduce the risk of a successful influence campaign because disinformation is usually born from a seed of truth," said Sönnergren, one of the consultants on the project.

The team of consultants began by interviewing election authorities from a handful of municipalities that were representative of the country with regard to size and resources. "We found that election administration was fairly similar across the municipalities," Sönnergren said. "Resources differ, and numbers of polling stations differ, but fundamentally, they all face the same risks and vulnerabilities. Everyone needs electricity, a functioning postal service, poll workers, and polling stations. So you really can identify best practices for the whole system."

From those interviews and the work the team of consultants had previously done for Stockholm, the team developed three general best practices for election security. Municipal authorities should (1) conduct risk and vulnerability analysis, (2) perform scenario-based exercises, and (3) ensure coordination and cooperation among the different agencies and offices within a municipality.

The MSB worked with the 4C Strategies consultants to build those three overarching best practices into a training package. The first piece called for each municipality to identify the risks and weaknesses in its election administration. The consultants had conducted such a study for Stockholm during a two-day workshop, and they condensed it into a self-guided process with a template that municipal workers could fill out themselves.

The training materials included recommendations for risk reduction in specific areas, including information influence that would:

1. Increase efforts of communicating to citizens about how the election is run.
2. Conduct awareness-raising training in the municipality.

3. Set up communication forums internally.
4. Coordinate with local media.
5. Make sure public communicators are active during the election.

Part of the analysis guided authorities through the election process—from setting up polling sites to conducting the vote, to counting ballots—and encouraged the authorities to think through the risks and contingencies at every step.

The second piece of the training called for authorities to deal with specific situations based on various scenarios. For example, one situation posited that a post on an online forum threatened an attack on a truck carrying ballot papers in the municipality. The participants then had to discuss what they would do, whom they would involve, and what they would need in order to deal with the incident.

The final best practice was coordination with other public and private entities and groups to prevent disinformation from taking root and spreading, as well as to mitigate other risks.-"Social media has changed, the climate and opened up more possibilities for negative information influence about an election," said Anna Nyqvist, head of the national Election Authority. "It's so much easier to spread a rumor about election fraud now. That means authorities need to cooperate more."

The training encouraged local election authorities to organize getting-to-know-you meetings with all the key stakeholders several months before the election and then host regular coordination meetings after that. "If all of these people know one another and talk to one another regularly, it's easier to stamp out false information and more quickly respond if there are problems," Sönnergren said.

The MSB sent the training package and an introductory video to all of the county administrative boards, which in turn sent them to all of the municipalities. In spring 2018, the MSB–4C Strategies team delivered the training in person to the election authorities from all 45 municipalities in Västra Götaland county. "It was an important tool," said Tofvesson. "It empowered the municipalities to gain knowledge of their own situations. Protection couldn't be centralized; it had to be decentralized. But no one out in the municipalities really had a national perspective, so this tool gave them that national perspective."

Coordination structures

The MSB worked to strengthen coordination at the national level by developing new structures and buttressing existing ones. "Coordination is essential because we have strong agencies, independent authorities, and not much hierarchy," said Nyhlin, a coordination expert at the MSB. "Maybe it's because we originated as a nation of farmers that owned their own land that it's so hard to tell anyone what to do."

The most important need for collaboration was between the bodies that ran the election and the bodies that secured it—two groups that in past elections had had little interaction. After Nyqvist pointed out the gap and raised the need for better coordination, the MSB, in partnership with the Swedish Security Service, set up a high-level forum that brought together the heads of the agencies in charge of *coordinating* the electoral process (the national Election Authority, the election authorities at the county administrative boards, and the Tax Agency, which supported the Election Authority) with the agencies in charge of *securing* the electoral process (the Swedish Police Authority, the Swedish Security Service, and the MSB).

The forum met for the first time in January 2018 and then roughly every month until the election. The first goal was to enable all of the leaders to get to know one another and to understand one another's roles and responsibilities. Then Bay led scenario-based discussions in which he would present a hypothetical election incident, such as a cyberattack or baseless allegations of election fraud, and then go around the table asking each agency how it would respond. The idea was that if there was a major influence operation or other kind of incident during the vote, the relevant players would have a better idea of what to do and whom to contact.

The sessions produced changes in how agencies thought about election security. The police, for instance, improved coordination with election authorities and adopted a new incident code covering election-related problems and threats.

The MSB created a parallel forum for communications and media officials from the agencies and authorities in order to plan public communications and prepare strategy for risk and crisis communication around the election.

Twice in 2018, the MSB convened national coordination meetings with about 40 government agencies to discuss the election, risks, contingencies, and the crisis management system. Representatives from Facebook and Twitter attended the meetings as well.

If a serious incident occurred during the election—say, a terrorist attack on several polling places or a major flood—the incident would be handled through the normal crisis coordination structure, which was bottom-up. The municipalities were responsible, but if the municipalities became overwhelmed, they could appeal to the counties for support and resources. And if the counties became overwhelmed they could appeal to the MSB, which could coordinate the pooling and deployment of national resources.

To maintain readiness, the MSB hosted every week an hourlong coordination conference call for all of the agencies that had crisis management responsibility—a group that included county administrative boards and others. (Each county administrative board hosted a similar meeting for its municipalities.) In the months leading up to the September 2018 vote, the election became an agenda item on the call so as to underscore that the participating groups were aware that managing election incidents—including a disinformation attack on the electoral process—would follow the same chain.

To aid with coordination, the MSB also compiled a comprehensive listing of the names and contact information of every person involved in conducting and securing the election. Anyone who attended an MSB-linked training or meeting was added to the list. "Having the phonebook meant that in any specific municipality, we would know who to talk to about vulnerabilities—someone who knew our way of thinking," said Tofvesson. The MSB maintained the master version, and a smaller edition was shared more broadly.

Moreover, during the election period, the MSB task force served as a clearinghouse for electoral disinformation incidents reported by municipal and regional election authorities. Using its power to require reporting from other agencies and authorities, the MSB sent a letter instructing every election authority to report election-related disinformation. An MSB analysis team would review incident reports to determine whether they were likely foreign interference activities. For those that were, the MSB would prepare a report and distribute it to relevant government agencies and to the county administrative boards, which in turn would distribute it to the municipalities.

Monitoring the information space

The analysis team on the MSB task force monitored online information sources financed and directed by foreign states that targeted information influence activities against Sweden. Examples were two Kremlin-backed media outlets, *Sputnik* and *RT*, which regularly directed propaganda at Sweden. In one well-publicized incident, a Russian TV crew attempted to bribe a group of Swedish teenagers to riot on camera to support a narrative that the government's migration policy was inflaming unrest.[6] (The full list of the sources the MSB monitored and the agency's methods for analyzing foreign influence were classified.)

Sweden's strong commitment to freedom of speech and privacy protections complicated the MSB's job. Although its analysts kept abreast of general "rumors and disinformation floating around in our information environment," as Tofvesson said, the agency did not analyze the channels or accounts generating or spreading them. "We have freedom of speech and the right to be anonymous when you use that freedom," he said. "The MSB therefore does not monitor social media accounts in general in search of foreign state actors hiding among our population, because that would risk monitoring and registering our own population."

Because of those constraints, the MSB turned to outside researchers to monitor social media. "We couldn't monitor the online political discourse, but we could fund academics to do it," said Bay. "One of our takeaways from the 2016 US election was that we didn't want to end up in a situation where no one was looking. No one there had been monitoring social media, and so no one really knew what had happened."

First, the MSB contracted the Swedish Defence Research Agency to monitor social media platforms and issue monthly updates ahead of the election. A government agency under the Ministry of Defence, the Defence Research

Agency's thousand or so personnel provided project-based research for the Swedish military, the police, and other national security and civil defense agencies.

The MSB contracted the agency in early 2018 for two projects: first, to monitor several social media platforms for conversation about threats to the election, and second, to identify and monitor the behavior of automated Twitter accounts (i.e., bots) focused on the election. Johan Fernquist, a researcher at the agency who had a background in computer science, was tapped to lead the project and assigned a part-time team of five to seven Defence Research Agency researchers with expertise in computer science, psychology, and social sciences. Before beginning the project, the team had to obtain permission from one of the six regional ethics review boards, which were state committees that imposed ethical guidelines on research involving human subjects, biological material, and personal data.

For the threat detection project, the team built web crawlers that gathered the texts of posts and comments on Facebook, Twitter, Instagram, and several other, similar platforms operating in Sweden, including Nordfront, a highly active extremist white nationalist site; *Social News* (*Samhällsnytt*), an antimigrant online magazine; and Flashback, the country's largest online discussion forum. The team ran automated searches throughout the text data for keywords related to the election and various threats to it that the team developed through conversations with the Election Authority and the police. The keywords were grouped by topics such as election fraud, physical attacks on polling sites, voting disinformation, election ballots, and the voting process. Those keywords formed the basis for signals showing the volume and distribution of threat conversation about the election.

On a regular basis—once every two weeks from March to May and then, after a summer break, every week in August and September before the election—the team hosted seminars attended by people from the MSB and other agencies and authorities working on the election. Presenters detailed which threat conversations about the election were drawing the most interest on each of the platforms and illustrated with charts and network maps which conversations were gaining traction with users. The reports also contained specific false stories that were being liked, shared, and commented on. "We were just reporting what people were talking about," said Fernquist. "We saw lots of conversations about vote buying, fraud in counting of the early vote, and voter intimidation at polling sites. A lot would originate from a single real or fake news article of a specific example that people would then amplify into claims of a systemic issue."

The second project involved the detection of election-focused bot networks on Twitter. The researchers downloaded all tweets about the election and developed a machine-learning program to identify bot accounts. A bot account was any that showed automated behavior—whether operated by software or a human. The researchers tracked the level of support on Twitter that the political

parties contesting the election received from bot accounts and from real accounts.

The team released results in a brief public report three weeks before the election. The results showed that populist far-right parties received the greatest share of support from bots. Bots had been widely reported features of the attack on the 2016 US election, so media interest in the report was high. "Everyone was afraid of bots because of the American election, and we could put numbers on how many there were," said Fernquist. "We couldn't say where the accounts originated from, but we did give a picture of what was going on." After the election, the team released a final report with its findings.[7]

In addition to the Defence Research Agency, the MSB contracted a team of four researchers from the London School of Economics and Political Science and the Institute for Strategic Dialogue, a United Kingdom–based research organization that focused on issues involving polarization, hate, and extremism. The researchers monitored international online information campaigns that aimed to influence the Swedish election and to damage Sweden's reputation abroad. The team included Peter Pomerantsev, a best-selling author and specialist in Russian propaganda, and Anne Applebaum, a Pulitzer Prize–winning journalist and historian with expertise in Soviet and contemporary Russian history.

To avoid monitoring the population on social media during the election period, the MSB instructed the research team not to share any of its results until after the election. The team's report, *Smearing Sweden: International Influence Campaigns in the 2018 Swedish Election,* was published shortly after the election.[8]

Coordinating with traditional and social media

In addition to researchers, the MSB enlisted the media to help monitor—and counter—disinformation. Ahead of the 2018 election, the MSB, along with the Election Authority, briefed, trained, and built relationships with journalists in the traditional news media and established partnerships with social media companies.

Television and the internet were the two primary sources of news. In 2017, 70% of Swedes reported obtaining news from television, and 86% from online sources, including 51% from social media.[9] Public trust in the large, mainstream news outlets was high. Public broadcaster Sveriges Television (SVT) was the most-watched and most-trusted news organization; in a Pew survey, 90% of respondents said they trusted SVT, and more respondents said it was their primary news source more than any other outlet was.[10]

As in most countries, online news and opinion sites outside the mainstream had proliferated in recent years. But such sites were not legitimate news outlets in the eyes of the state. Newspapers, either print or digital, that complied with certain government-set criteria received subsidies under a legislative framework established in the 1960s to prevent newspaper closures and media consolidation that would stifle editorial diversity.[11] The Swedish Press and Broadcasting Authority, an independent government regulator, determined who qualified.

Even with the advent of the internet, Sweden had one of the highest rates of newspaper circulation in the world, and most towns had at least two competing news dailies.

In contrast to established newspapers and media, Swedes expressed little trust in online sources. One survey found only 12% of Swedish Facebook users thought most of the information on Facebook was trustworthy.[12]

After the 2016 US presidential vote, electoral information influence became a hot topic in the Swedish media. News organizations increased the rigor and granularity of their coverage of the election and information influence, and several hired data journalists, invested in education for journalists and staff, and funded investigations into troll farms and other disinformation subjects. SVT, Radio Sweden, and three of the country's largest newspapers partnered to create Faktiskt.se, an initiative for the fact checking of statements issued by politicians during the campaign season.

Four times a year, the MSB convened the country's main news outlets—those that adhered to accepted journalistic practices—in the Media Preparedness Council, a forum on media security and emergency support. At the meeting in fall 2017, the MSB raised the issue of information influence targeting the election and discussed what the role of the media was and how the MSB could provide support. "We told them that neither the MSB nor any other government agency was monitoring the web to identify and debunk political manipulation around the election. It was up to them. They were our best defenses," said Bay.

An MSB official who was a former chief editor at a newspaper reached out to the editorial boards of media outlets and newspapers to offer briefings on the information influence threat against the election. Emma Sjöblom, a senior administrator at the Election Authority, joined the MSB official to explain to journalists and editors the details of how elections were run and any changes in the election law, and to dispel common misunderstandings about the election, such as about early voting and party registration. "Journalists sometimes inadvertently spread fake news about the election because they had misunderstandings about the electoral process," Sjöblom said. "If we trained journalists to understand how the process worked, then that meant the public would better understand how it worked."

The MSB–Election Authority team made presentations to a dozen newsrooms, and some were attended by as many as 100 journalists, editors, and staff. The presentations were often held over lunch so as to encourage attendance. The team also filmed a lecture and distributed it through a network of freelance journalists.

Sjöblom said many of the journalists who attended the presentations contacted her during the election period to check factual aspects of articles about the election. "That proactive outreach we did with the lectures was important," she recalled. "Journalists work on deadline, and they immediately knew I could answer questions about the election. I ended up straightening out several mistakes in articles about the election before they were published, and I don't think that would have happened if we hadn't had those lectures."

In addition to traditional media, the MSB also developed what Bay described as "very good working relationships with social media companies." Agency workers met with representatives from Facebook, Google, and Twitter. Facebook in particular was an important partner because it was the most-used social media platform and the top platform for news; of the 51% of Swedes who said they obtained news from social media, 70% said Facebook was their main source.

In late 2017, the MSB reached out to Facebook's office in Stockholm and met with the company's public policy representatives for Sweden. The MSB's request of Facebook was to ask not that the company remove any content from the platform but only that it prioritize requests to review accounts or pages that were falsely purporting to be election authorities. "I think they were used to governments asking them to remove content, so it took several times of our saying we were not asking them to remove content before they realized what we were asking for was quite limited and easy to do," said Bay.

Facebook agreed. The company and agency established a direct support line through which the MSB could directly report false election authority accounts. When a Facebook page falsely purporting to be the election authority of the city of Göteborg appeared on the platform, the MSB used the support line, and Facebook removed the page.

Facebook also cooperated with the Swedish Election Authority. No less than three times during the 2018 election period—first when early voting abroad began, then when early domestic voting began, and just before election day—Facebook published public service announcements on users' news feeds with a link to the Election Authority's website. "We saw traffic on our website was much higher on the dates when they ran those announcements," said Election Authority head Nyqvist.

Raising public awareness

In the months before the election, Tofvesson and other members of the MSB made several media appearances to raise public awareness about the threat of information activities targeting the election, especially the vulnerabilities that disinformation would seek to exploit.

At first, Tofvesson said, his message to the public was to think critically about information regarding NATO, migration issues, or Russophobia. A common Kremlin-driven narrative was that Sweden's government unfairly maligned Russia. After a month, however, he realized that he should take into account not only the full breadth of potential topics of disinformation but also the emotional aspects of how disinformation aimed at sowing chaos and eroding trust. "A defining feature of fake news is that it evokes an extreme, emotional response," said Tofvesson. "Our message became, 'If you see something that makes you really happy or really upset, then think critically about the source of the information.'"

The MSB knew the communications strategy had to convey confidence as well. "Talking about a risk can scare people," Nyhlin said. "But you need to have

experts out there communicating that risk actively because the worst thing is to seem as if you're covering something up or lying. But if you deliver a message about a risk, you also need to talk about the system in place to handle that risk."

The greatest source of assurance was Nyqvist, whom others described as having an air of competence, authority, and credibility. She made frequent media appearances to deliver a simple, consistent message: The election was robust because it was manual, decentralized, and transparent. "Anna Nyqvist was the most important communicator," recalled Nyhlin. "We arranged for her to appear on a popular morning news show alongside Tofvesson, and she was on a big radio program with leaders from the MSB and Security Service. Linking her with the country's top crisis officials was good; it illustrated that the election was secure."

Several initiatives outside the MSB election defense project sought to help the public identify and disregard disinformation. The MSB revived the publication of a civil defense brochure called *If Crisis or War Comes*, a 20-page pamphlet containing basic information about what to do in case of a war or national emergency. Some form of the brochure had been published and mailed to every Swedish household beginning in 1943, in the middle of World War II. Distribution ended in 1991, when the Cold War ended, but in 2018, the MSB published an updated version of the brochure and sent it to 4.8 million Swedish households. The new version included discussions of cyberattacks and terror attacks and told how to recognize and deal with fake news and other disinformation.[13]

In March 2017, the Swedish government announced a nationwide reform in elementary and high school curricula whereby it would add lessons in how to recognize fake news. It instructed the Swedish Media Council, a government agency, to develop teaching materials, which were completed in 2018 and incorporated into public school curricula.

OVERCOMING OBSTACLES

The weeks leading up to election day on September 9, 2018, were largely without incident. The logistical preparations for voting had gone smoothly, and the early voting period proceeded without disruption. On election day itself, however, two situations caught the MSB by surprise. And though neither disrupted the process nor significantly damaged its credibility, both revealed vulnerabilities the agency had not anticipated.

The first involved a cyberattack on the Election Authority's web page that showed real-time vote results on the night of the vote. The attack left the site inaccessible for about four hours. Forensic analysis later showed that a single hacker had used Tor, an open-source software that facilitates anonymous online activity, to exploit a flaw in a website. Investigators said the attack, which lacked the sophistication of a coordinated or state-directed operation, had had no impact on the vote because the site did not hold the actual vote result.

Bay said he and others at the MSB weren't worried at first. After all, for the past several years, major news channels and newspapers had had direct access to

the election IT infrastructure that enabled them to obtain and publish the vote results themselves. As a result, most Swedes watched the results on TV or visited newspaper websites. "I thought, 'So what if the Election Authority site was down? It doesn't matter, as people had access to the election results anyway,'" Bay said. "That was a flawed cognitive assessment."

Accusations of fraud quickly sprang up on social media, including allegations that the site's outage somehow reflected a plot to steal votes from one party and give them to another. "None of it went very far because the media didn't pick up the story, but it became a storm in a teacup for a little while," said Bay.

The second situation arose when the Election Authority encountered a flood of media requests regarding homegrown disinformation on social media. Party supporters posted or tweeted allegations of fraud or mismanagement, and journalists who saw the content contacted the authority to request comment or clarification for how to handle it.

Thanks in part to the lectures the Election Authority had delivered to news outlets, the reporters knew whom to call, but the high call volume overwhelmed the authority's small staff. "We had no idea how massive the interest from the media would be," said Nyqvist. "Lots of it was driven by rumors or baseless allegations on social media." Press requests continued to flood the Election Authority communications staff for a week after the vote.

Although few of the reports were credible and none of the incidents disrupted the election, the experience demonstrated the need to better prepare the Election Authority for the 2022 election. The MSB began developing a plan to bolster the authority's communications staff with people from other agencies during the election. Additional plans called for improving the speed of incident reporting by municipalities, where most incidents occurred, to enable the Election Authority get in front of similar situations before they could spread through the public domain.

ASSESSING RESULTS

Based on his analysis of monitoring efforts conducted by both the MSB task force and the outside researchers at the Swedish Defence Research Agency and the London School of Economics and Political Science and Institute for Strategic Dialogue team, Tofvesson concluded that there was no coordinated foreign influence operation against the 2018 Swedish election. The attack on the Election Authority's website and other incidents were minor, isolated, and likely homegrown, and they did not disrupt the electoral process or substantively damage its credibility. In all, 87.5% of eligible voters cast ballots—the highest turnout since 1985.

The MSB task force received only 20 disinformation-incident reports from the municipal and regional election authorities—far fewer than the hundreds or even thousands Tofvesson was anticipating. Every case originated from a homegrown source—except for one interference activity tied to Hizb ut-Tahrir, an international fundamentalist Islamic organization seeking to establish an

Islamic caliphate. Because the group's social media posts urged Swedish Muslims not to vote, a form of electoral interference, the MSB created a report and disseminated it to all county administrative boards for them to distribute to municipalities.

In its final report, the research team from the London School of Economics and Political Science and the Institute for Strategic Dialogue determined that although international far-right and Russian state-sponsored media had promulgated propaganda and disinformation designed to damage Sweden's reputation, there was no internationally managed or coordinated influence campaign. The most consistent disinformation narrative was the claim of election fraud intended to disenfranchise Sweden's far-right parties.[14]

It was difficult to determine whether the preparations the MSB had made would have enabled the system to withstand a disinformation campaign of the kind that hit the US election. "We did all this preparing and all this interagency coordinating and communicating, but we were never really tested," Nyhlin acknowledged.

The preparations had indeed been extensive. MSB training—delivered either in person or through materials delivered for self-instruction—reached as many as 14,000 civil servants and election administrators. Feedback and anecdotal evidence suggested the training was valuable. The Lund University–MSB team conducted evaluations of the training sessions they held with public communicators. That included surveys that participants filled out immediately after the training that contained questions about whether it was useful and helped them feel more empowered to identify and rebut disinformation.

"The results were fantastic," recalled Pamment. "Everyone loved the training. That doesn't necessarily mean everything in it worked in the field, but the methods were based on best practice from the social scientific community." He added that demand for the training was high. "Municipalities in the middle of nowhere were asking for the MSB to come out and train their staffs. That's evidence that this was valuable."

The 4C Strategies consultants, too, received positive feedback from the elections protection training they provided for municipal authorities. "The municipalities we were responsible for training were very appreciative," said Sönnergren. "They used the training, and it was relevant—super relevant. There was a major need for best-practice materials." Sönnergren reported that election authorities had followed recommendations in the training. "In following up with some of the municipalities we trained, we learned many municipalities did indeed hold regular coordination meetings before and during the election period," he said. One shortcoming, however, was that many of the smaller municipalities lacked the capacity to conduct the recommended risk and vulnerability analysis. In its preparations for the 2022 election, the MSB complemented the recommendation by also issuing guidelines for mitigating election risks.

Another measure of success was international appropriation of the MSB's strategy and methods. Several countries adopted the handbook for communicators, and Pamment conducted training sessions with a dozen other

countries. Nations in Scandinavia and the Baltic region, especially, looked to Sweden as a model. Finland, for instance, emulated Sweden's resilience-building strategy for defending its own elections, along with several of the specific practices.

An open question was whether foreign actors took note of Sweden's preparations and were deterred from launching an attack. "Did we deter aggression? I don't know, maybe," said Bay. "I think the whole democratic world doing these kinds of things probably deters aggression, because it has been getting more and more difficult for antagonists to do the exact same thing they did in 2016 again."

Yet even though there was no coordinated foreign-influence campaign against the Swedish election, homegrown disinformation flooded the media landscape. Researchers at Oxford University's Oxford Internet Institute analyzed 275,000 tweets about the Swedish election over a 10-day period in August. They found that one in every three articles shared was from a junk news site—that is, an outlet that deliberately publishes "misleading, deceptive or incorrect information purporting to be real news."[15] The vast majority of that junk news supported right-wing politics, particularly on issues related to migration and Islam.

In the election, the Sweden Democrats, a far-right populist party, won 17.5% of the vote—its best showing to date—though short of expectations established in opinion polling. Still, the party became the third largest in parliament.[16]

There was no way to prove whether all that disinformation had influenced voters' preferences. "I think it did have an impact, but to what extent is the question," said Hanna Stjärne, CEO of SVT. "I don't think it did to such a great extent."

REFLECTIONS

By late 2020, Swedish leaders and policy makers had recognized that disinformation had become a permanent feature of modern political discourse. "This is a problem we will have to live with," said Hanna Stjärne, chief executive of public broadcaster Sveriges Television. "We will have to continue to be aware of the problem and how it changes, but the best vaccine we could have is resilience: the ability for as many people as possible in our society to think critically about sources and fact-check information."

Swedish society had features that made a resilience-building approach more likely to succeed. The tradition of civil and psychological defense—that every Swede had the responsibility to resist foreign invasion or influence, information or otherwise—predisposed the Swedish public and institutions to understand and accept the approach.

Popular and trusted public media provided reliable information. Even before modules specifically about identifying fake news were added to public education curricula in 2018, schoolchildren learned critical thinking and the ins and outs of political propaganda.

Sweden had strong cultural defenses against the fundamental goal of disinformation: to undermine trust in institutions and government. For decades, Swedish institutions had enjoyed relatively high levels of public trust, and that trust held firm in the face of the influx of fake news. Public opinion surveys showed that trust in Swedish institutions remained relatively high. In a survey of Swedish public opinion by the University of Göteborg's Society, Opinion and Media Institute, confidence in the police, courts, and armed forces in 2019 was the highest it had been since the annual survey was first conducted in 1986. Confidence in political parties and the government was slightly lower than it had been in the early 2010s, but the deviation from the multiyear average was minor.[17]

In its work, the Swedish Civil Contingencies Agency (*Myndigheten för samhällsskydd och beredskap*, or MSB) benefited from full-spectrum political commitment. The prime minister and other leading politicians spoke and wrote publicly about the importance of defending the election against disinformation. "Some countries have struggled on this issue from a lack of political commitment," said Sebastian Bay, a member of the MSB Counter Influence Unit. "Here, all the government agencies supported our work. Not once did someone say, 'Why would we need to defend the election?' People agreed elections are good and that we should do what we can to protect them."

After the 2018 election, the government doubled down on its whole-of-society, resilience-building approach to defending the election. As part of a shift in national security policy to revive the total defense doctrine, the government approved the creation of a new psychological defense agency that would support other agencies by means of communications and information matters. As of late 2020, the proposal detailing the parameters of the new agency was being reviewed by other agencies in a process required for creating a new arm of government. It was expected that the Counter Influence Unit at the MSB would become a central part of the new agency.

References

[1] "Assessing Russian Activities and Intentions in Recent US Elections." US Office of the Director of National Intelligence, January 6, 2017; https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[2] Craig Timberg, "Russian propaganda may have been shared hundreds of millions of times, new research says." *Washington Post*, October 5, 2017; https://www.washingtonpost.com/news/the-switch/wp/2017/10/05/russian-propaganda-may-have-been-shared-hundreds-of-millions-of-times-new-research-says/.

[3] Reuters Institute Digital News Report 2017. Reuters Institute for the Study of Journalism, 2017; https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202017%20web_0.pdf.

[4] James Pamment et al., *Countering Information Influence Activities: The State of the Art*. MSB and Lund University, July 2018; https://www.msb.se/RibData/Filer/pdf/28697.pdf.

[5] James Pamment et al., *Countering Information Influence Activities: A Handbook for Communicators*. MSB and Lund University, July 2018; https://www.msb.se/RibData/Filer/pdf/28698.pdf.
[6] Robbie Gramer, "Russian TV Crew Tries to Bribe Swedish Youngsters to Riot on Camera." *Foreign Policy*, March 7, 2017; https://foreignpolicy.com/2017/03/07/russian-tv-crew-tries-to-bribe-swedish-youngsters-to-riot-on-camera-stockholm-rinkeby-russia-disinformation-media-immigration-migration-sweden/.
[7] Johan Fernquist et al., *Bots and the Swedish election: A study of automated accounts on Twitter*. Swedish Defense Research Agency, September 2018; https://www.foi.se/rest-api/report/FOI%20Memo%206466.
[8] Chloe Colliver et al., *Smearing Sweden: International Influence Campaigns in the 2018 Swedish Election*, London School of Economics and Political Science and Institute for Strategic Dialogue, November 2018; https://www.isdglobal.org/wp-content/uploads/2018/11/Smearing-Sweden.pdf.
[9] Nic Newman et al., *Reuters Institute Digital News Report 2017*. Reuters Institute for the Study of Journalism, 2017; https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202017%20web_0.pdf.
[10] Pew Research Center, "News Media and Political Attitudes in Sweden." May 17, 2018; https://www.pewresearch.org/global/fact-sheet/news-media-and-political-attitudes-in-sweden/.
[11] Karl Erik Gustafsson et al., "Press Subsidies and Local News: The Swedish Case." Reuters Institute for the Study of Journalism, September 2009; https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2017-11/Press%20Subsidies%20%26%20Local%20News%20the%20Swedish%20Case.pdf.
[12] Svenskarna Och Internet - Valspecial 2018. Internetstiftelsen i Sverige, 2018, https://internetstiftelsen.se/kunskap/rapporter-och-guider/svenskarna-och-internet-valspecial-2018/.
[13] *If Crisis or War Comes* (English version), Swedish Civil Contingencies Agency, 2018; https://www.dinsakerhet.se/siteassets/dinsakerhet.se/broschyren-om-krisen-eller-kriget-kommer/om-krisen-eller-kriget-kommer---engelska-2.pdf.
[14] Chloe Colliver et al., *Smearing Sweden: International Influence Campaigns in the 2018 Swedish Election*, London School of Economics and Political Science and Institute for Strategic Dialogue, November 2018; https://www.isdglobal.org/wp-content/uploads/2018/11/Smearing-Sweden.pdf.
[15] Jack Stubbs and Johan Ahlander, "Exclusive: Right-wing sites swamp Sweden with 'junk news' in tight election race." Reuters, September 6, 2018; https://www.reuters.com/article/us-sweden-election-disinformation-exclus/exclusive-right-wing-sites-swamp-sweden-with-junk-news-in-tight-election-race-idUSKCN1LM0DN?utm_source=twitter&utm_medium=Social.
[16] Reid Standish, "Meet Sweden's New Populist Kingmakers," *The Atlantic*, September 10, 2018; https://www.theatlantic.com/international/archive/2018/09/sweden-democrats/569743/.
[17] *Swedish Trends: 1986-2019*, eds. Johan Martinsson and Ulrika Andersson, University of Gothenburg SOM Institute; https://www.gu.se/sites/default/files/2020-06/7.%20Swedish%20trends%20%281986-2019%29_v2.pdf.

Innovations for Successful Societies makes its case studies and other publications available to all at no cost under the guidelines of the Terms of Use listed below. The ISS Web repository is intended to serve as an idea bank, enabling practitioners and scholars to evaluate the pros and cons of different reform strategies and weigh the effects of context. ISS welcomes readers' feedback, including suggestions of additional topics and questions to be considered, corrections, and how case studies are being used: iss@princeton.edu.

Terms of Use

Before using any materials downloaded from the Innovations for Successful Societies website, users must read and accept the terms on which we make these items available. The terms constitute a legal agreement between any person who seeks to use information available at successfulsocieties.princeton.edu and Princeton University.

In downloading or otherwise employing this information, users indicate that:

a. They understand that the materials downloaded from the website are protected under United States Copyright Law (Title 17, United States Code). This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/.
b. They will use the material only for educational, scholarly, and other noncommercial purposes.
c. They will not sell, transfer, assign, license, lease, or otherwise convey any portion of this information to any third party. Republication or display on a third party's website requires the express written permission of the Princeton University Innovations for Successful Societies program or the Princeton University Library.
d. They understand that the quotations used in the case study reflect the interviewees' personal points of view. Although all efforts have been made to ensure the accuracy of the information collected, Princeton University does not warrant the accuracy, completeness, timeliness, or other characteristics of any material available online.
e. They acknowledge that the content and/or format of the archive and the site may be revised, updated, or otherwise modified from time to time.
f. They accept that access to and use of the archive are at their own risk. They shall not hold Princeton University liable for any loss or damages resulting from the use of information in the archive. Princeton University assumes no liability for any errors or omissions with respect to the functioning of the archive.
g. In all publications, presentations, or other communications that incorporate or otherwise rely on information from this archive, they will acknowledge that such information was obtained through the Innovations for Successful Societies website. Our status and that of any identified contributors as the authors of material must always be acknowledged and a full credit given as follows:

Author(s) or Editor(s) if listed, Full title, Year of publication, Innovations for Successful Societies, Princeton University, http://successfulsocieties.princeton.edu/