Global Challenges
Election Disinformation

INNOVATIONS FOR SUCCESSFUL SOCIETIES

DEFENDING THE VOTE: ESTONIA CREATES A NETWORK TO COMBAT DISINFORMATION, 2016–2020

Tyler McBrien drafted this case study based on interviews conducted in September and October 2020. Case published December 2020.

SYNOPSIS

Troubled by reports of disinformation and fake news in the United States and with regard to the United Kingdom's Brexit referendum vote, Estonia's State Electoral Office in 2016 created an interagency task force to combat the influence of false messaging on its democratic process. To guide its work, the small staff of the State Electoral Office adopted a network approach by engaging partners from other government agencies, intergovernmental organizations, civil society, social media companies, and the press to identify and monitor disinformation and to work with the press to correct false statements. It also developed a curriculum that would help high school students improve their ability to separate fact from fiction. The collaboration largely succeeded in checking foreign interference. However, considerations involving free speech and censorship hobbled the task force's efforts to restrain disinformation spread by domestic political parties and their supporters. This case illuminates how an electoral management body with limited staff capacity and a restricted mandate addressed a societywide disinformation challenge.

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

In late 2016, more than 4,000 miles from Washington, D.C., Priit Vinkel read with interest—and some trepidation—about attempts to influence the recent US presidential election. Groups connected to Russia had spread false or misleading information on social media and Russian state media channels in an attempt to foment distrust in the electoral system.[1] "2016 was a warning for us," said Vinkel, head of Estonia's State Electoral Office. "After we followed the US elections, there was a shared feeling among our different institutions that we needed to do more."

Vinkel was well acquainted with a range of attacks aimed at undermining the integrity of his own country's electoral process. He had worked since 2007 in Estonia's electoral management body—an independent office with discretion over its own budget—and had led the institution since early 2013. But Vinkel now recognized a new threat in the form of disinformation: the intentional spread of false information in order to influence public opinion and weaken public trust in government. Such interference threatened many facets of Estonian society, such as support of Estonia's participation in the NATO alliance, but elections were high-value targets.[2]

Situated between Latvia, Russia, and the Baltic Sea, Estonia gained independence from the Soviet Union in 1991, establishing itself as a parliamentary representative democratic republic, with a prime minister who served as head of government and a term-limited, indirectly elected and largely ceremonial president. At the time, less than half the population had phone lines, but Estonia rapidly went digital, eventually distinguishing itself as a leader in government technology through an initiative known as e-Estonia.[3] In 2005, it became the first country in the world to offer its citizens an option to vote via the internet.

Two years after achieving that milestone, however, Estonia acquired another distinction when it fell victim to the world's first coordinated, large-scale cyberattack. The government had relocated a Soviet-era World War II memorial known as the Bronze Soldier—a monument of importance to many of the country's Russian-speaking residents, who constituted about 30% of the country's 1.3 million inhabitants. The move, which angered members of that Russian minority and which was already dissatisfied with growing postindependence inequality, sparked mass protests in Estonia's capital, Tallinn. Following the unrest, three weeks of denial-of-service attacks disabled government, banking, and media websites.

Although the source of the attacks was never identified with certainty, observers in Estonia and around the world mostly agreed that Russia was to blame. Russian state media routinely engaged in influence campaigns aimed largely at Estonia's ethnic Russian minority and sometimes tried to widen fissures between Russian speakers and the Estonian majority.[4]

In the years after the attack, Estonia shored up its cyberdefenses and fortified vulnerable computer networks, including the internet voting system that facilitated online balloting. "The cybersecurity game was upped enough for it

not to be worthwhile for the adversary anymore," said Liisa Past, who served as Estonia's chief national cyberrisk officer in 2019 and 2020. "Cyberattacks grew to be expensive, and strong defenses by no means meant you were guaranteed success."

But as disinformation and so-called fake news grew increasingly sophisticated around the world—and with local elections scheduled for 2017 and national and European parliamentary elections in 2019—defending the vote from such a complex new threat became a central task for Vinkel and his small team at Estonia's State Electoral Office.

THE CHALLENGE

Before taking on the challenge of disinformation, Vinkel had to define the boundaries of the problem. The idea itself—the propagation of falsehoods aimed at achieving a political goal—was nothing new. But what was once considered relatively innocuous rumormongering or political truth-stretching had morphed into something more sinister for Estonia and other democracies. Elections were prime targets, as demonstrated by the 2016 US presidential vote and the Brexit referendum. Social media had become a powerful force in citizens' lives because it enabled disinformation to reach a far wider audience while anonymizing the disinformation's origins (text box 1). "The US experience was something to learn from, but in the Estonian case, one topic was even more at the center of our discussions: trust in the election management organizations—specifically through the internet voting process and the presentation of correct preliminary election results," Vinkel said.

Text Box 1: Defining Disinformation

Finding and defining disinformation was difficult because modes of disruption evolved rapidly. In addition, sources of disinformation and misinformation were difficult to discern. Trolls, hackers, and government agents intentionally obfuscated certain information's origins, and bots proliferated the information anonymously. The spread of disinformation also existed on a spectrum of severity, ranging from someone unknowingly sharing a falsified news story on a social media channel to a coordinated attempt to hack into a country's election results web page and replace it with a similar website broadcasting inaccurate election results.

Several labels and definitions existed for false or misleading information. Some countries, such as Malaysia and Russia, defined terms like *disinformation* and *fake news* through legislation. Estonia had no legal definition of any of those terms, but it did have an operational one for disinformation, modeled after the European Union's interpretation. Siim Kumpas, who worked in the strategic communications unit of the Government Office, said Estonia broadly defined *disinformation* as "false or misleading information that is created and spread intentionally for either political, economic, or personal gain." The Estonian government avoided using the terms *fake news*, *false information*, and *misinformation* because those terms tended to not distinguish between intentional manipulation of information and human error or satire.

Even if the State Electoral Office identified false information related to elections, such as a spurious news article claiming the internet voting system had been hacked, the Estonian government had distinct hurdles to overcome. Because its democratic constitution protected free speech, both the government and the citizenry had long accepted the idea that domestic politicians and their supporters often spread false or misleading information. Foreign media outlets were free to operate newspapers, radio stations, and television networks within the country. Plus, the government could place few restrictions on Russian state-sponsored media outlets, which were popular among Estonia's Russian-speaking minority and were often accused of dispersing so-called fake news and disseminating pro-Kremlin propaganda.

Lack of a legal and operational framework was another challenge. Vinkel said no laws, rules, or regulations existed that could assign government responsibility and authority to deal with attempts to influence elections through disinformation campaigns. The country's constitution set up a semi-presidential parliamentary system that vested the power to administer elections in the National Electoral Committee and a network of election managers and polling staff, organized by the State Electoral Office.[5] Although the office was housed in parliament, it maintained a separate budget and remained independent and apolitical. The responsibilities of the State Electoral Office included any actions needed to "ensure the holding of the elections in accordance with law," organization of electronic voting, supervision over election managers' activities, and the development and management of technical solutions, such as the election information system and the electoral results web page.[6]

Estonia's election administrators traditionally were careful not to overstep those specific activities. "The legal-driven world of election management is terribly suited for the sort of dynamic, comprehensive risk management required to combat disinformation," said cyberrisk officer Past. "Election organizations like to say, 'Our mandate ends here.'"

Limited capacity in the State Electoral Office presented another challenge. Vinkel had neither the tools nor the personnel at his disposal to monitor Estonia's information environment—including traditional television and radio channels as well as several social media platforms—and effectively track down disinformation. In 2016, the office had just 10 full-time staff members and lacked the expertise required to handle the problem. "You can't expect someone who runs elections maybe once a year or every 18 months to have both cybersecurity and communications expertise in-house," said Past. At the time, software that automatically tracked the spread of social media postings was rudimentary.[7]

In addition to its small staff and limited capacity, the State Electoral Office had a mandate that restricted its activities to elections, meaning that it had to rely on the expertise and work of other government agencies and outside groups. Election disinformation often got mixed with other messaging about Estonia's foreign policy and domestic policies with regard to the country's Russian minority—topics that were beyond the State Electoral Office's sphere of

influence. The need to coordinate across government, private-sector, civil society, and international organizations posed an ongoing challenge, and the office had to figure out how to manage those relationships—whether formally or informally.

Because effective action against disinformation required the active cooperation of social media providers, the government also had to develop partnerships and direct lines of communication with private companies that had headquarters around the world. Such companies were global platforms like Facebook and Twitter, both of them based in California, and Russian-language platforms like VKontakte (VK), based in neighboring Russia. With its modest population and low profile in the international community, Estonia faced an uphill climb to establish leverage with the firms.

FRAMING A RESPONSE

Recognition of the importance of communications when it comes to defense priorities had grown steadily in Estonia during the previous few years. In 2014, Estonia and several allies established the NATO Strategic Communications Centre of Excellence in neighboring Latvia due to the growing prevalence of information influence operations.

In 2016, as Vinkel contemplated how to approach Estonia's particular challenge, the country's parliament and prime minister had nearly finished drafting the National Security Concept, which updated the objectives, principles, and strategies of national security policy. The document ranked strategic communications as one of six broad development areas for national defense, defining it as "planning the state's political, economic and defence-related statements and activities, preparing a comprehensive informative whole on the basis of these, and transmitting it to the population" and identifying its main objective as "the resilience and better cohesion of society."[8]

To Vinkel, combating externally generated election disinformation was an important dimension of the issues the Concept covered. Although Vinkel had no explicit legal framework for correcting the problem and with the 2017 local elections only months away, he interpreted the State Electoral Office's mandate to include protection from disinformation. That interpretation was not far beyond the usual responsibilities of the office, which often fought what Vinkel called "PR battles" against misconceptions and false narratives about the security of internet voting.

Countering disinformation was still a relatively new field, and Vinkel had few established strategies from which to draw. He recognized, however, that success would require active participation by other government agencies and departments—capitalizing on the government's willingness to apply agile principles and to let people take on new responsibilities—at least temporarily.

Seeking ideas, Vinkel and others in the State Electoral Office visited their counterparts in Norway, Sweden, Finland, and Latvia. Sweden in particular was a leader in this field, drawing on a World War II–era tradition of psychological defense.[9] Sweden's national security doctrine also espoused total defense,

whereby every citizen prepared for war or crisis and wherein the government developed educational, training, and exercise programs to help Swedes identify and resist propaganda and information warfare. "The Swedish model was clearly in front of us, as was the US experience," Vinkel said. But the State Electoral Office had far less capacity than Sweden did to carry out such an aggressive strategy. "They did everything as a survival exercise," Vinkel said. "But we didn't have the resources to take it to that level. We had to do it as clean and lean as possible."

Empowered by the mandate of his office to convene officials across the government and with informal approval by other officials, Vinkel began to put a system in place. He decided that Estonia needed a unified government response: an ad hoc, interagency working group called the election communications task force. The task force's mandate broadly included any messaging related to elections—such as how to reach Estonian voters living abroad—but disinformation was the group's primary focus.

To populate the task force with the specialists he needed, Vinkel aimed to use what he called a *network* approach. "The defining characteristic here was cooperation," said Vinkel. "The election management body in a small-scale system cannot rely on its own capability and has to gather other specialist institutions. This does not mean that the different nodes of expertise should act on their own but, rather, through the election management body as the main focal point."

The election communications task force consisted of members of the Government Office, the Information System Authority, the Ministry of Foreign Affairs, and the Ministry of the Interior. Vinkel said the two pillars of the group were the Government Office and the Information System Authority. The Government Office was similar to the United Kingdom's Cabinet Office by its support of the prime minister and the cabinet with policy planning and implementation, cabinet meetings, public relations, and legal compliance. The Information System Authority, which managed and protected the state's internet network and ensured secure e-elections, had worked with the State Electoral Office since internet voting debuted in 2005.[10] The Ministry of Foreign Affairs played a less important role in the task force—by communicating accurate election information to the small number of Estonians voting from abroad—and the Ministry of the Interior assisted in monitoring the internet for disinformation.

The Government Office's strategic communications team was the natural partner to coordinate and lead most of the work because of its significant capacity and broad purview. Siim Kumpas, a strategic communications adviser with the Government Office who worked closely with Vinkel and the State Electoral Office on disinformation, described strategic communications as "all communication activities that support the long-term aims of your institution, including words, actions, and symbols." Kumpas said that although the Government Office was run by the secretary of state—an appointee of the

prime minister—the office was "apolitical in essence" because it was a part of the civil service.

In late 2016, Vinkel began to lay the groundwork for the interagency task force on election communications, as well as for separate working groups dedicated to cybersecurity and election technology infrastructure. At first, it was an uphill battle to persuade other agencies to join. "The other institutions thought that elections were not their concerns," Vinkel remembered. Behind the scenes, though, he built on past relationships and made personal appeals to technical experts at the Government Office, the Information System Authority, and several ministries. Vinkel and his partners also appeared before parliament's constitutional committee to deliver a briefing on the newly formed task force, even though they were not legally obligated to do so. "The agencies had been part of our inner circle before, but never in this type of format," said Vinkel. "We had consulted people in other agencies on specific matters, but this was the first time cooperation was forged on a more institutional level as an interagency task force."

Vinkel established nonbinding "goodwill cooperation agreements" with the State Electoral Office's two closest collaborators: the Information System Authority and the Government Office. The Government Office loosely formalized its relationship with the State Electoral Office by providing a list of services its people would provide. "The cooperation started off fairly ad hoc, but we formalized it to the minimum extent needed to work together so that both sides understood what to expect and what to give," said Kumpas. "That was the framework; it wasn't anything overtly official. In essence, it was a list of services we were able and mandated to offer them" (text box 2).

The approach was possible in part because of the government's overall willingness to allow units to share responsibilities in order to adapt and respond to changing circumstances. "Our systems have to be much more flexible than in

Text Box 2:
List of Services Provided for State Electoral Office by the Government Office

Following is a list of services provided by the strategic communications unit.

- Building systematic, working-level relations with most of the important tech platforms in Estonia (i.e., Facebook, Google, Twitter, Microsoft)
- Monitoring the information sphere—including both Russian media and Estonian social media—and compiling weekly reports on common disinformation narratives
- Compiling a hands-on guide for political parties and the general public with regard to how to recognize and deal with information attacks
- Briefing journalists and editors on risks related to and posed by foreign informational interference
- Mapping risks related to the election process in partnership with the State Electoral Office and the Information System Authority
- Amplifying the State Electoral Office's communication initiatives through official Government Office channels

some bigger countries because a lot of people here have quite a lot of different roles," Kumpas said. His ability to work with the State Electoral Office on the election disinformation threat while also handling strategic communications in the Government Office is an example of that policy.

Establishing interagency working relationships was one thing, but generating the will to cooperate and coordinate was another. To persuade agencies to participate, Vinkel pointed to the National Security Concept, the government strategy paper that identified psychological defense, which was defined as "informing society and raising awareness about information-related activities aimed at harming Estonia's constitutional order, society's values and virtues" as an indispensable aspect of keeping Estonians safe.[11] At that time, the cabinet had already approved the National Security Concept, and parliament would approve it just months later, in May 2017.

GETTING DOWN TO WORK

In April 2017, six months before the local vote, the election communications task force convened its first meeting. It planned to meet weekly at first and then increase the frequency of meetings to twice weekly during the two months before elections.

Identifying the nature of the threat

One of the first items on the agenda was to scrutinize the nature of the information influence challenge that Estonia confronted. Such scrutiny was essential for guiding the resources and efforts of the task force moving forward. Although there was widespread acknowledgment within the government with regard to the threat posed by disinformation operations, no comprehensive risk analysis existed.

Past recalled that during one early task force meeting, she felt troubled by what she thought was too narrow a cybersecurity view of the threats and risks to Estonia's electoral system. "I realized that when talking about risk management, it was all technical risks within the IT systems," said Past, who served as the Information System Authority's chief research officer for cybersecurity at the time. "The technical risks are clear, and, frankly, easier to mitigate. But it also became increasingly evident that threats existed across strategic communications, information operations, and cybersecurity."

After urging the group to take a more comprehensive view, Past's director general tapped her to conduct an initial threat analysis. By interviewing people across the government, Past worked to analyze the information (text box 3). Past's threat analysis was broad ranging. Peddlers of disinformation often exploited the ethnic fissure that existed between the Russian minority and the Estonian majority—a strategy that echoed back to the relocation of the Bronze Soldier, which had led to Bronze Night and the 2007 cyberattacks.

In Estonia, Russian speakers received most of their information from television, and the most-popular Russian-language stations were controlled by Moscow. That meant that the Russian government could easily broadcast

Text Box 3: Strategic Communications Election Security Preparation

In June 2019, experts at the NATO Strategic Communications Centre of Excellence published *Protecting Elections: A Strategic Communications Approach*, which mapped out the following questions for electoral management bodies protecting elections from disinformation.

1. Information landscape: What is the situation we are in, and what are we protecting?
   - What are the core elements of Estonia's information environment and its election process?
   - How do voters make decisions?
   - What are the aspects of the information environment and voting process we most want to protect?
2. Threat assessment: What is the nature of the threat?
   - What are the publicly recognized security risks to and vulnerabilities of elections?
   - How could activities aimed at influencing information and swaying public opinion take shape?
   - What are the likelihood and consequences of those activities?
   - Which risks do we have to accept for our context?
3. Risk and capability assessment: How do we handle the identified risks?
   - How can we reduce the probability and consequences of election information interference?
   - What is our monitoring capability?
   - What are the deterrence mechanisms at our disposal?
   - What are the mechanisms through which we will coordinate our response?

election disinformation directly to the Russian minority in Estonia. And because previous attempts to break the Kremlin's monopoly on Russian-language media had fallen flat, the Estonian government in September 2015 launched a Russian-language station called ETV+; but the fledgling station struggled to attract viewers away from the better-resourced, better-produced Russian stations.[12]

Although traditional media outlets also sometimes blurred the distinction between legitimate information and disinformation, internet-based social media posed an especially nettlesome problem for Estonian government officials. Disinformation circulated on global platforms Facebook and Twitter as well as popular Russian-language social media websites VKontakte and Odnoklassniki. One report from the NATO Strategic Communications Centre of Excellence estimated that VKontakte and Odnoklassniki had 327,000 and 250,000 Estonian users, respectively, making them even more popular than Facebook in some parts of the country.[13]

Even with a high level of societal trust in the technology used in the country's elections, internet voting was a potential target for anyone aiming to undermine trust in the Estonian electoral system. "One of our fears was that internet voting would be low-hanging fruit to whoever wants to question the integrity of our electoral system as a whole," Kumpas said.

Despite those vulnerabilities, Past said, the analysis she completed in early 2017 determined that Estonia's electoral process faced little threat from foreign disinformation operations. Still, Vinkel said he felt that disinformation had the potential to undermine voter confidence in Estonia—especially with regard to internet voting, for which Estonia had gained an international reputation. At the same time, Vinkel's partners in other government agencies were becoming more enthusiastic in their acknowledgment of disinformation as a threat worth tackling.

The initial threat analysis became a living document that all members of the task force could update with input from their individual findings and recommendations.

Monitoring the information sphere

After the task force better understood what it was looking for, monitoring both traditional media and social media for election disinformation became a primary task. Vinkel said he came to rely heavily on human partners in the Government Office, the Information System Authority, civil society, and the media because automated monitoring services and so-called bots that comb online media channels for indications of disinformation were insufficient. "It was, as is quite often the case in Estonia, a cooperation between the Government Office and several other institutions and agencies," said Kumpas. "We each played a small part in the media or social media ecosystem that we kept an eye on and analyzed. And then we in the Government Office were the ones to pull it together and share with the electoral office."

Media monitoring benefited from the network approach. Kumpas oversaw the Government Office's social media watchers, who kept an eye on thousands of social media channels and flagged potentially harmful disinformation. Even though its mandate was limited to cybersecurity, the Information System Authority contributed. While combing cyberspace for malware, phishing scams, and other potential threats to the country's computer infrastructure, the authority's analysts would flag suspicious posts that contained specific words and phrases such as "Estonia elections" or "i-voting." At meetings of the election communications task force, participants reviewed data from various sources and decided whether and how to respond to certain false news stories. Typical discussions involved questions about how to handle a story in some faraway newspaper that claimed Estonia's e-voting system was insecure.

Lauri Tankler, the Information System Authority's lead analyst, explained that his agency's people, who monitored cyberspace around the clock, were on the front lines. "We were looking at the Estonian threads on forums, chatrooms, Reddit, and social media. Nothing extensive, but enough to actually see where some rumors or disinformation may start out as smaller pieces of chatter. There's always a sequence. Before it jumps to social media and the public sphere, disinformation gathers steam on more private platforms, including the dark web" (parts of the internet that were accessible only by means of special software or with authorization).

Tankler stressed that the role of the Information System Authority was to uncover instances of suspected disinformation—such as i-voting conspiracy theories or wrongful information about voting dates—and report them "in a way that could be understood by the State Electoral Office and the Government Office," which would decide whether to take action.

Vinkel, Kumpas, and other members of the task force often looked to Propastop—an independent blog run by volunteers guided by the Ministry of Defense—for analysis of pro-Kremlin news media websites. Beginning in 2016, Propastop volunteers, who worked anonymously because of concerns about possible harassment and retribution, published articles to a blog refuting common online information influence campaigns and narratives. Most Propastop content focused on Russia because according to the organization's website, "the Bronze Night, the Russo-Georgian War, the Annexation of Crimea and the support of eastern Ukraine have gone hand-in-hand with intense propaganda and information attacks."[14]

Propastop volunteers maintained a symbiotic relationship with investigative journalists in Estonia by collaborating on content creation, sharing resources and information, and republishing articles relevant to Propastop's mission and findings. For example, one Propastop post in September 2018, titled "Will the Estonian elections be influenced as well?" promoted stories by investigative journalists in Estonia and abroad to expose the objectives and likely methods that would be used to influence Estonia's elections ahead of the European and national parliamentary elections the following March.[15] *Postimees*, Estonia's oldest and most widely circulated newspaper, often republished the full text of Propastop blog posts. The blog also ran media literacy campaigns and training for journalists.

Every week, the State Electoral Office compiled reports from the agencies and organizations that hunted for election-related disinformation and e-mailed a media-monitoring summary to all members of the election communications task force. Task force members then used the reports to inform their strategies for public messaging on official social media channels and public service announcements.

Establishing partnerships with social media companies

Vinkel said that between the 2017 and 2019 elections, he wanted to expand the task force's capability to monitor and combat election disinformation on social media. Even though the group was powerless to censor or remove most instances of election disinformation because of free-speech protections, the group could appeal directly to social media platforms to do so if certain posts violated their own company policies. But first, the task force had to establish working relationships with the companies.

Vinkel felt it was important to maintain streamlined communications, so he asked Kumpas and the Government Office to take the lead as the main points of contact. Kumpas said he took a local approach rather than try to deal with executives at the far-flung headquarters of giant corporations that operated in

Estonia, including Twitter, Facebook, Google, and Microsoft. Instead, he worked with the companies' regional representatives to set up direct lines of communication, which he called *hotlines* or *red phones*. "We didn't try to use our diplomatic channels to approach their higher executives," Kumpas recalled. "We approached from the working level to find the right people to talk to."

Kumpas placed special emphasis on Facebook, whose users included the highest number of Estonian voters. The relationship was tested in December 2018, just months from national elections in March and European parliamentary elections in May, when Propastop analysts and an investigative journalist, Holger Roonemaa, uncovered more than a hundred suspicious Facebook accounts (a significant number for a country with a small population) and a group called Estoners. By digging into personal information listed on the Facebook profiles, Roonemaa and Propastop proved that the administrators of the Estoners group had used fake profiles, and Roonemaa and Propastop published a story about it online. Kumpas seized on the story, added his own analysis and input from the task force, and sent a report of their findings to his contacts at Facebook.

"Even though their processes are not transparent, to put it mildly, Facebook took all of the accounts down and eventually closed the group," said Kumpas. "It proved to be a good test for seeing whether our link with the social media platforms worked or not. And second, it was a good example of the network approach, which can sound like a vague buzzword." The move appeared to be part of a larger crackdown at Facebook against what the company termed "coordinated inauthentic behavior." In January 2019, Facebook closed more than 350 pages and accounts associated with a Russian state-owned media company across the Baltics, eastern Europe, and Central Asia.[16]

Enlisting international organizations and other countries

Estonia's network approach reached beyond its borders. "Cooperation with like-minded countries is essential," said Kumpas. "It's repeated often, but information operations know no borders, so we have to share with like-minded countries all of the data, experiences, lessons learned, and mistakes made." Given the common information influence threat perceived by the Baltic and Nordic states, Estonia looked to its neighbors and allies for strategies that could be adapted to the Estonian context. Estonia also shared its own successful strategies to maintain its reputation as a "poster child of digital transformation," according to Past, and to deter potential antagonists planning information influence campaigns.

In December 2018, Estonia welcomed the European Union's Action Plan against Disinformation, which described activities to be taken by the East StratCom Task Force, established in 2015 to address Russia's disinformation campaigns.[17] East StratCom's three objectives included communication and promotion of EU policies in the so-called Eastern Neighborhood (Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine), supporting media freedom and strengthening independent media organizations, and improving the EU's

capability to forecast, address, and respond to disinformation by external actors.[18]

The group regularly published articles on a website called EUvsDisinfo.eu, which collected by 2019 nearly 10,000 examples of pro-Kremlin disinformation in 20 languages. The election communications task force monitored EUvsDisinfo.eu for disinformation aimed at Estonia's elections, finding disinformation cases on EUvsDisinfo.eu that contained a summary of the false claim, information on where the claim was published, and evidence disproving the claim.

"If you're trying to discuss Russian disinformation, then you need examples as proof or evidence," said Madis Vaikmaa, a former journalist from Estonia who joined the East StratCom Task Force, where he ran the EUvsDisinfo.eu website and database with five colleagues. "We now have thousands of these examples. We're gathering them to show that pro-Kremlin media outlets are spreading disinformation, and it's still a problem that must be fixed" (figure 1).


DISINFO: ESTONIAN E-VOTING IS NOT SECRET AND HAS BENEFITED SPECIFIC PARTIES

SUMMARY

Voting over the Internet in recent years has been beneficial primarily to the right-wing parties.

In 2013, a 89-year-old retired woman took part in the elections to the board of the Reform Party. She did not own a computer and she also did not know how to use one.

There is no secret voting – in 2011, a 58-year-old Tallinn resident voted 553 times via the Internet and the representatives of the election commission called her to explain that only one vote would be counted.

DISPROOF

According to the Freedom of the Net 2018 report, "The Estonian e-governance system is one of the most advanced in the world." Also, the Estonian e-voting system has nothing to do with the system used by the Reform Party.

According to the report by the University of Tartu, e-voting could mobilize new voters and people of higher socio-economic status who are more likely to lean to the right of the political spectrum. "The only plausible explanation for the aggregate level differences in party vote tallies depending on the mode is therefore that a large share of typical voters have simply switched from paper voting to e-voting and this process is non-random, meaning a larger share of supporters of particular parties have done so. Should e-voting be discontinued, these people would simply switch back to paper voting", the report said.

In 2011 the Estonian Information System Authority, State Electoral Office and police discovered an anomaly caused by mass voting connected to a single IP-address. Although the voting is secret, the Estonian Information System Authority can make sure who is behind an (accidental) attack to the system and thus the lady was indeed contacted.

Go to search

Facebook Twitter

PUBLICATION/MEDIA
→ RIAFAN - Russian (Archived)

REPORTED IN:
Issue 135

DATE OF PUBLICATION:
29/01/2019

LANGUAGE/TARGET AUDIENCE:
Russian

COUNTRY:
Estonia

KEYWORDS:
Manipulated elections/referendum

DISCLAIMER

Cases in the EUvsDisinfo database focus on messages in the international information space that are identified as providing a partial, distorted, or false depiction of reality and spread key pro-Kremlin messages. This does not necessarily imply, however, that a given outlet is linked to the Kremlin or editorially pro-Kremlin, or that it has intentionally sought to disinform. EUvsDisinfo publications do not represent an official EU position, as the information and opinions expressed are based on media reporting and analysis of the East Stratcom Task Force.

Figure 1. *https://euvsdisinfo.eu/report/e-voting-has-benefited-right-wing-parties/*

In March 2019, the European External Action Service, the European Union's diplomatic service, launched the Rapid Alert System, which shared with all EU member states all information and research on common disinformation campaigns. Each member state appointed a single contact person who disseminated the alerts throughout the contact person's member state government. The Rapid Alert System used open-source information, combining research from academia, fact checkers, and vetted news sources.[19]

Investing in public education and media literacy

To educate the public about disinformation, Kumpas began by publishing a hands-on guide for officials in both the public and private sectors. Looking again to his neighbor across the Baltic Sea, Kumpas adapted a handbook written by experts at Lund University and the Swedish Civil Contingencies Agency to fit the Estonian context. "The original handbook was meant for communication professionals, but we wanted to adapt ours for a wider audience," said Kumpas. "So we stripped everything nonessential to fit it on nine pages." The Government Office made the guide available online for the general public, and it organized training for public servants in ministries and agencies (text box 4).

Text Box 4:
Highlights from the Government Office's Disinformation Handbook

Published in early 2019, *A Guide to Dealing with Information Attacks* was modeled after a similar handbook written by the Swedish Civil Contingencies Agency and Lund University. "The Estonian state operates in a decentralized manner, which means that each ministry and agency is responsible for what is happening in its own backyard," the introduction began. "This also applies to information advocacy. We have agencies who systematically keep an eye on this topic, but we all need to be able to deal with individual cases ourselves to cope. The purpose of this guide is to provide basic tips for recognizing disinformation and (if necessary) to respond to it." The guide contained the following sections.

1. Preparing for disinformation attacks
    a. Identifying vulnerabilities and raising awareness
    b. Preparation of narratives and messages
2. Responding to disinformation attacks
    a. Assessing the situation
    b. Informing the public and key partners
    c. Proactive communication
    d. Retaliation
3. Common methods of influence
4. Identifying bots
5. Tips for responding to unfamiliar journalists

Adapted from *Countering Information Influence activities: A Handbook for Communicators*, Swedish Civil Contingencies Agency; msb.se/RibData/Filer/pdf/28698.pdf.

Members of the task force used their relationships with journalists and chief editors at Estonia's largest newspapers and media houses to reach a wider audience. "We held frequent meetings with journalists to give them all the basic election information so they could have a quick rebuttal if something came up that wasn't true," Vinkel said. The Government Office also organized training for journalists, again using the network approach. At the training sessions, representatives of the State Electoral Office explained the nuts and bolts of election administration; people from the State Information Authority described the threat of cyberattacks and how election cybersecurity worked; and others from the Government Office revealed possible information influence operations and described the risks associated with those attacks.

In 2019, the Estonian government also began to invest more funds in public education. The Ministry of Education and Research, in collaboration with the European Commission, organized an awareness-raising Media Literacy Week. The campaign's motto was "Think before you share" and included a series of online videos featuring popular journalists.[20] The ministry also instituted a compulsory, 35-hour course called Media and Manipulation for high school students. The course covered media basics such as the various kinds of media products, the difference between opinions and news, a definition of who

is considered a journalist, a definition of social media, and the different rhetorical methods used for swaying opinion.

OVERCOMING OBSTACLES

Although the task force's team approach dealt effectively with the foreign disinformation threat, the curbing of internal election meddling proved to be an elusive goal. Ahead of both the 2017 and 2019 elections, political activists spread false information about the security of Estonia's internet voting system. Tankler, of the Information System Authority, said the situation had involved opinions and misinformation that were "propagated by supporters of mainly one specific Estonian political party and activists who are inherently against online voting." He stressed that analysts saw no "credible foreign interference attempts in our elections."

Officials from the State Electoral Office, the Government Office, and the Information System Authority said they felt it was both outside their mandate and unethical to contest any claims made by Estonian politicians or their supporters because doing so would appear to be a partisan move that would diminish the trust Estonian voters placed in their state institutions. And in an effort to remain impartial, Propastop focused solely on outside influence attempts. "It should be noted that propastop.org does not engage itself in creating propaganda," the organization explained on its website. "It restricts itself only to exposing propaganda. We also respect the right to freedom of speech for every Estonian citizen, including difference of opinions about Estonia."[21]

Members of the election communications task force debated how to address internal disinformation threats. "We were analyzing what we could and couldn't do within our mandate," said Kersti Luha, who was with the Government Office's strategic communications unit with Kumpas. "But ultimately, we concluded our mandate was for foreign interference and not internal debates on political questions. We understood that media literacy and education of the electorate are key in these questions, but that they were also a bit separate from securing elections."

By the end of the 2019 election cycle, the election communications task force was still puzzling over the tension between disinformation and freedom of expression. "The biggest disinformation question we have in Estonia is how to deal with the freedom of speech or the freedom to lie," said Tankler. "Of course we try to correct mistakes that are put out on social media, but we're not going to be actively present in every single Estonian Facebook group where people with strong opinions promote any bit of information or misinformation they find to discredit this process."

ASSESSING RESULTS

Measuring the effectiveness of Estonia's efforts to counter disinformation presented a daunting challenge for the task force. Vinkel said there was no reliable way to measure disinformation's true influence on a population, and

there was no way to effectively monitor all outlets and sources of potential disinformation. Kumpas agreed: "Everyone's trying to figure out how to measure success and the impact of failure, but I don't think either of those questions has really got definitive answers."

In the absence of strong metrics, the Government Office conducted opinion surveys and focus groups from October to December 2019 to better understand public perceptions about false information. The survey designers intentionally avoided the word *disinformation* because it was not a household term in Estonia. Over half of surveyed Estonian residents either agreed or strongly agreed to the statement, "It's easy for me to identify false information." Similarly, 56% of respondents agreed or strongly agreed they "often notice false information in the media." And 50% either agreed or strongly agreed that the same applied to social media. And in December 2019, Eurobarometer, a series of public opinion surveys conducted by the European Commission, found that the share of Estonians who said they felt they often encountered fake news or disinformation had increased more than the share in any other EU country from September 2018 to September 2019.[22]

Significantly, only a small proportion of respondents in the Government Office's surveys said disinformation had much effect and was a matter of concern. About 13% agreed or strongly agreed that false information published in the media and social media negatively affected their lives, and 24% agreed or strongly agreed that false information in the media changed the attitudes or behaviors of their relatives or friends.

In lieu of solid evidence that the Estonian public considered disinformation to be a significant threat, the Government Office saw a need for more education on how to respond to false information. Analysts found that survey respondents said they more commonly responded to false information identified online by ignoring it or deliberately sharing it because it was amusing rather than by responding in more constructive ways such as verifying it with more-reliable sources, informing social media platforms of its existence, or commenting on a post or news story to refute it.

Overall, despite progress against foreign information influence, such as the case of Facebook's removal of the Estoners' fake accounts, Kumpas remained cautious about drawing conclusions about the role of social media in the recent elections. "It was not clear that the accounts would have had any kind of tangible effect on the outcome of our elections," he said. "Our assessment was that the risk of an effective information operation targeted from abroad against our elections was pretty low, and in the end, it turned out to be correct." Measuring an increase or decrease in the spread of disinformation on social media proved especially challenging. "It's a problem all over the world," said one Propastop analyst. "You can count your page followers and post views, but you can't see what the algorithm is doing or how many people actually see a post. It's completely dark."

One of the chief goals of disinformation campaigns, especially Russian ones, was to discourage citizens from voting by eroding the perceived integrity

of Estonia's electoral system and state institutions. In the Government Office's public opinion surveys conducted in 2019, 63% of respondents said they trusted the information transmitted by official channels of state agencies. Vinkel and other officials also viewed the country's high and growing percentage of votes cast online as a proxy for citizens' degree of trust in the electoral system. In the 2019 national parliamentary election, 247,232 votes—representing nearly 44% of the total—were cast online.[23] That marked a 40% jump from the 186,034 i-votes cast during the previous election, according to website e-Estonia.[24]

Outside evaluators also took notice. The Open Society Institute of Bulgaria, a nongovernmental organization based in Sofia, ranked Estonia 5th out of 35 European countries in its Media Literacy Index, which assesses countries' resilience to fake news, degree of media freedom, public education, and trust.[25]

In its final report after Estonia's 2019 parliamentary elections, the Organization for Security and Co-operation in Europe, a Vienna-based intergovernmental group that regularly observes national balloting, found that "the campaign took place in an environment characterized by high citizen trust in public institutions." The observers wrote, "Election authorities continued to enjoy broad stakeholder confidence and were commended for their independence and professionalism."[26]

However, the observers also drew attention to persistent challenges, noting the possibility of future "significant risks that may negatively affect public confidence in Internet voting," including cyberattack allegations from disinformation campaigns or human error.[27]

REFLECTIONS

Asked for his advice to other countries that are fighting disinformation, Siim Kumpas, a strategic communications advisor in the Government Office who led much of the task force's anti-disinformation portfolio, said it was important to put Estonia into context. "We understood, having seen what happened in the United States in 2016 and in several other places, that it would be wise to pay extra attention to disinformation," Kumpas said. "But I would argue that Estonian people are a bit more accustomed to this kind of informational influence, given our geographic positioning and historical background. So, the thinking itself wasn't novel, but applying this thinking to election integrity was a first for us."

Kumpas also stressed that Estonia's small population worked in the country's favor. "The Estonian language serves as a kind of shield against foreign interference, because it's spoken by only about a million people all over the world," he said. "So it's really hard to find someone who speaks fluent Estonian and is willing to use that against Estonia."

Despite Estonia's distinctive features, Kumpas felt that his country could offer transferable lessons to democracies facing similar threats. "First, I would say that Estonia's network model proved itself," he said. "For future elections, we could formalize the relationships between government institutions a bit more, but not too much. As a small country, we need to remain flexible." The

International Institute for Democracy and Electoral Assistance (IDEA), an intergovernmental organization based in Stockholm, also praised Estonia's network model: "Many countries have a single task force on election cybersecurity, yet Estonia has found that a model with several small, focused groups is more effective."[28]

An important step toward formalization would be for other agencies to draw up similar lists of services offered to the State Electoral Office the way the Government Office had done in the run-up to the 2019 elections. Rather than being simply a strategy of necessity, this network approach produced clear benefits. A report published by IDEA in 2019 explained that in Estonia, "interagency collaboration takes place through multiple ad hoc task forces and working groups. Splitting collaboration into task forces allows groups to remain small, focused and effective. Task forces work based on personal, professional contacts while working groups are usually conducted between designated representatives of various organizations."[29]

Second, Kumpas felt that thorough understanding of a country's specific media and information landscape was essential. "Monitoring the media and having situational awareness are prerequisites to getting ready for standing against information attacks," he said. "If you don't see and understand what's happening around you, everything after that becomes kind of a gamble. If you want to prevent information attacks against elections, set up a good media monitoring system, and, if possible, run public opinion surveys that give you the data you need."

Priit Vinkel, who led Estonia's State Electoral Office from 2013 until taking paternity leave in 2020, agreed. "The most important thing we learned was that when we don't have information on what's happening on social media, we're running into the battle blind," he said.

Constant social media monitoring was labor- and time intensive, but several companies had promising automated technologies in development. In 2018, Propastop, an independent anti-propaganda blog run by anonymous Estonian volunteers, launched Propamon, a monitoring robot that flagged news related to Estonia in the Russian media.[30] The same year, an Estonia-based start-up called Sentinel began to develop a platform for the Estonian government and the European Union to automatically detect disinformation by using data from common disinformation campaigns.

Third, Kumpas stressed the importance of establishing strong partnerships with social media companies. "Relations with social media platforms have to be in place well before elections," he said. But establishing such lines of communication, especially with Facebook, was easier said than done, and Vinkel and Kumpas identified that point as a target for improvement for future elections. "Although we got most of what we wanted, we ideally would have wanted more openness from the social media companies," said Kumpas. "If we take the example of the fake accounts mentioned earlier, it would have been useful to understand the people targeted, affiliated parties, and engagement rates." Legislation and regulation could have made the task force's job easier, but

Kumpas recognized that Estonia's problem was not unique. "It doesn't make much sense that countries have to rely on the mercy of a handful of social media companies in order to protect their electoral integrity, but at the moment, this is the case," he said.

Unresolved questions regarding freedom of speech, censorship, and domestic disinformation lingered. Democracies around the world faced the same difficult questions. Madis Vaikmaa, an Estonian journalist who served as a strategic communications expert with the European Union's task force on Russian disinformation, said that he often asked himself, "What do you do when information is technically true, but the underlying message is to suppress the vote?" Estonia's commitment to free speech meant that the country would always remain vulnerable to information attacks—at least until someone developed a workable solution.

"Any rumor or disinformation campaign about how Estonian elections can be hacked puts the Information System Authority, Government Office, and State Electoral Office immediately in a defensive position," said Lauri Tankler, a lead analyst in Estonia's Information System Authority. "Having to refute claims made is already a losing position, which may undermine voter confidence."

In the end, Estonia's long-standing dedication to earning public trust buttressed the entire system and served as the first line of defense against disinformation. "In the case of Estonia, the strict impartiality of the country's state institutions, the government, and the election management bodies has a central, critical role," said Ingrid Bicu, a specialist in strategic communications and elections at the International Institute for Democracy and Electoral Assistance. Maintaining that perception of impartiality required a high degree of trust in government.

Liisa Past, who served as Estonia's chief national cyberrisk officer, said Estonia maintained that trust through "radical transparency and aggressive openness" not only in elections but also across all areas of e-Estonia.

The Estonian government's understanding of disinformation was still evolving well after the 2019 elections wrapped up. In late 2020, the Government Office planned to meet with the Estonian Language Institute—a national cultural institution promoting the standardization and survival of the Estonian language—to review a list of 40 terms related to disinformation, including *misinformation* and *deepfakes* (images or videos altered to deceive viewers). Kumpas said he hoped to add such terms to the Estonian language database as one more step toward understanding the threat posed by disinformation.

References

[1] *Report of the Select Committee on Intelligence, United States Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 1: Russian Efforts against Election Infrastructure with Additional Views*. United States Senate; https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.
[2] Oliver Backes and Andrew Swab, "Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States," Harvard Kennedy School Belfer Center for Science and

International Affairs, November 2019; https://www.belfercenter.org/sites/default/files/2019-11/CognitiveWarfare.pdf.
[3] "How Did Estonia Become a Leader in Technology?," *The Economist,* July 31, 2013; https://www.economist.com/the-economist-explains/2013/07/30/how-did-estonia-become-a-leader-in-technology.
[4] Todd C. Helmus et al. *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*. RAND Corporation, 2018; https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf.
[5] Composition, Competence and Functions of the National Electoral Committee. State Electoral Office of Estonia; https://www.valimised.ee/en/electoral-organizers/composition-competence-and-functions-national-electoral-committee.
[6] Sam van der Staak and Peter Wolf, *Cybersecurity in Elections: Models of Interagency Collaboration*. International Institute for Democracy and Electoral Assistance, 2019; https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf.
[7] "What's the Plan If Trump Tweets That He's Won Re-election?" *New York Times,* September 27, 2020; https://www.nytimes.com/2020/09/27/opinion/social-media-trump-election.html.
[8] "National Security Concept 2017." Ministry of Defence of Estonia; https://www.kaitseministeerium.ee/en/objectives-activities/basic-national-defence-documents, 19-20.
[9] Niklas H. Rossbach, "Psychological Defence: Vital for Sweden's Defence Capability." *Strategic Outlook 7*, FOI Memo 6207, November 2017; https://www.foi.se/rest-api/report/FOI%20Memo%206207#:~:text=The%20psychological%20defence%20activities%20of,in%20to%20a%20limited%20extent.
[10] "Introduction and Structure." Information System Authority of Estonia; https://www.ria.ee/en/information-system-authority/introduction-and-structure.html.
[11] "National Security Concept 2017." Ministry of Defence of Estonia; https://www.kaitseministeerium.ee/en/objectives-activities/basic-national-defence-documents.
[12] Alexandra Wiktorek Sarlo, "Fighting Disinformation in the Baltic States." Foreign Policy Research Institute, July 6, 2017; https://www.fpri.org/article/2017/07/fighting-disinformation-baltic-states/.
[13] Dmitri Teperik et al. *Virtual Russian World in the Baltics: Psycholinguistic Analysis of Online Behaviour and Ideological Content among Russian-Speaking Social Media Users in the Baltic States*. NATO StratCom Centre of Excellence, January 2020; https://www.stratcomcoe.org/virtual-russian-world-baltics.
[14] "What Is Propastop?" Propastop blog, March 6, 2017; https://www.propastop.org/eng/2017/03/06/what-is-propastop/.
[15] "Will the Estonian Elections Be Influenced as Well?" Propastop blog, September 18, 2018; https://www.propastop.org/eng/2018/09/18/will-the-estonian-elections-be-influenced-as-well/.
[16] Indra Ekmanis, "(De)friending in the Baltics: Lessons from Facebook's Sputnik Crackdown," Foreign Policy Research Institute, January 31, 2019; https://www.fpri.org/article/2019/01/defriending-in-the-baltics-lessons-from-facebooks-sputnik-crackdown/.
[17] *Action Plan against Disinformation*. European Commission, December 5, 2018; https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf.
[18] "Questions and Answers about the East StratCom Task Force." European Union External Action Service, December 5, 2018; https://eeas.europa.eu/headquarters/headquarters-Homepage/2116/questions-and-answers-about-east-stratcom-task-force_en.
[19] "Rapid Alert System." European Union External Action Service, March 2019; https://eeas.europa.eu/sites/eeas/files/ras_factsheet_march_2019_0.pdf.
[20] "Media Literacy Week 2020." Ministry of Education and Research of Estonia; https://www.hm.ee/et/MPN.
[21] "What Is Propastop?" Propastop Blog, March 6, 2017.

[22] "Special Eurobarometer 503: Attitudes towards the Impact of Digitalisation on Daily Lives," Eurobarometer, March 5, 2020; 43-47.
[23] Liisa Past and Keith Brown, "Attacks against Elections Are Inevitable – Estonia Shows What Can Be Done." *The Conversation*, March 28, 2019; https://theconversation.com/attacks-against-elections-are-inevitable-estonia-shows-what-can-be-done-109222.
[24] Juvien Galano, "I-Voting – the Future of Elections?" E-Estonia, March 2019; https://e-estonia.com/i-voting-the-future-of-elections/.
[25] "The Media Literacy Index 2019: Just Think about It." Open Society Institute Sofia, November 29, 2019; https://osis.bg/?p=3356&lang=en.
[26] *Estonia Parliamentary Elections ODIHR Election Expert Team Final Report*. Organization for Security and Co-operation in Europe, March 3, 2019; https://www.osce.org/files/f/documents/8/e/424229.pdf, 1.
[27] *Estonia Parliamentary Elections ODIHR Election Expert Team Final Report*. Organization for Security and Co-operation in Europe, March 3, 2019; https://www.osce.org/files/f/documents/8/e/424229.pdf, 9.
[28] Sam van der Staak and Peter Wolf, "Cybersecurity in Elections: Models of Interagency Collaboration." International Institute for Democracy and Electoral Assistance, 2019; https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf.
[29] Sam van der Staak and Peter Wolf, "Cybersecurity in Elections: Models of Interagency Collaboration," International Institute for Democracy and Electoral Assistance, 2019; https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf, 59.
[30] "Propamon: A New Robot Searching for Propaganda." Propastop blog, April 10, 2018; https://www.propastop.org/eng/2018/04/10/propamon-a-new-robot-searching-for-propaganda/.

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/.