www.globalcyberalliance.org

GLOBAL ELECTIONS SECURITY REPORT

April 2023

CROWDSTRIKE

GLOBAL CYBER ALLIANCE

International Foundation for Electoral Systems

Background

Election cybersecurity is an important element of democratic resilience. Malicious actors have identified cyberspace as an instrument of power and use cyber-attacks as a key method to achieve their aims across a spectrum of intentions, from causing general chaos to changing specific electoral outcomes. Elections around the world are being impacted to different degrees. While commercial and non-profit entities have already devoted considerable efforts to increasing cybersecurity for elections, governments remain the most important actors in preventing and mitigating election cyber-attacks. However, information technology is used across the entirety of an election cycle and is owned, maintained, and used by a variety of actors - software to hardware providers, candidates, and other institutions that play a role in election administration. And because the activities performed across the electoral process are interrelated, security compromises or breaches to one stakeholder can have wide-reaching effects. For all these reasons, we need a comprehensive, whole-of-society approach to election security.

It is with this in mind that the Global Cyber Alliance (GCA), supported by CrowdStrike and the International Foundation for Electoral Systems (IFES), launched a series of multi-stakeholder roundtable discussions. A few one-to-one interviews were also conducted. In total, forty-one leaders from sixteen countries, representing a broad range of sectors, participated. The discussions focused on the United Kingdom, Europe, and Asia Pacific and were divided into four sub-topics: technology, policy, collaboration, and skills and resources. They highlighted the importance of a broad approach to election security and identified challenges and best practices that are summarised in this report.

Acknowledgments

This report was prepared by the Global Cyber Alliance, with Ms. Kayle Giroud, Associate Director for Partnership & Sustainability, as the lead author. The report was supported by CrowdStrike and the International Foundation of Elections Systems (IFES) and benefited tremendously from contributions by Mr. Philip Reitinger, Mr. Brian Cute and Ms. Renee McLaughlin, Global Cyber Alliance, Dr. Tarun Chaudhary, IFES, Dr. Armin Rabitsch, Election-Watch.EU, Mr. Omri Press, Alliance4Europe, Mr. Giorgi Iashvili, Cyber Trust, Mr. David Levine, Alliance for Securing Democracy at the German Marshall Fund, Mr. Daniel Dobrygowski, World Economic Forum, and from all the participants in the roundtables and all the listed initiatives. The team is grateful to those individuals who reviewed various drafts and provided valuable insights. Funding for this project has been graciously provided by CrowdStrike, and a special thanks goes out to Mr. Robert Sheldon and Ms. Karen Kaya who made this project possible.

Executive Summary

This report takes an in-depth look at what cybersecurity players are doing to protect the integrity of elections around the world, from fighting the spread of false information which might prevent voters from forming opinions based on accurate information to securing voter data and election results from manipulation attempts.

This report offers ten recommendations to improve the cybersecurity of elections with a whole-of-society approach. Governments, industry, political parties, media, civil society, non-profit organisations, and citizens themselves all have a role to play in collectively improving the integrity of our elections.

Key Results

While online security resources are available, they remain often inaccessible to election management bodies (EMBs) in many parts of the world due to budget and other constraints. They need resources and the deployment of accessible tools and solutions.

Serious effort is needed globally to improve the cybersecurity awareness of participants in the election cycle, including civil society organisations, media, political parties, and citizens.

Table of Contents

The Way Forward: Recommendations

Policy

1/ Take a holistic approach to election security

As demonstrated by the ACE Project Electoral Cycle developed by the European Commission, International IDEA, and the UNDP, elections consist of a continuous set of interrelated sub-processes that take place before and after the act of voting occurs and involve a diverse set of stakeholders. When looking at the use of technology in elections, we need a holistic approach to the process and to not merely focus on the actual voting, which is only one particular portion of the election process. The election cycle comprises many actors such as political parties, the media, civil society, industry vendors, service providers, and so forth.

2/ Adopt and implement appropriate legislation and policies to promote cybersecurity and threat information sharing

Examples of collaboration exist at the government level between EMBs, law enforcement, and CERTs. However, the degree of formality for this collaboration varies greatly. In general, the necessity for EMBs to remain independent and avoid institutional capture by executive bodies, while relying on outside resources to gain access to robust cybersecurity, is a real tension that needs to be overcome. In order to be sustainable, collaboration should be formalised and guided by legislation and sound policy. Cybersecurity is often considered an IT topic with limited understanding of cybersecurity policy and governance at the EMB level. This results in ad-hoc approaches that are reactive instead of proactive management of cybersecurity risks. Lack of governance leads to lack of organisational structure and the absence of holistic cybersecurity capacity. Election managers require a degree of independence, and when reliant on outside ministries or agencies for cybersecurity capability, election managers must protect against undue institutional capture or influence.

Good practice

Australia has confronted the problem of maliciously registered domains distributing malinformation about elections and candidates. To register a domain within the .au ccTLD, all registrants must submit an application which is validated by the registrar against a reliable and independent electronic database (such as the Australian Business Register at: https://abr.business.gov.au/) to ensure the individual or political party is legitimate. The administrator for the .au ccTLD, .au Domain Administration Limited (auDA), also monitors keywords that may be used in a political campaign and can highlight domain names for further investigation.[1] While this is good practice, replicating it may vary from one country to another depending on data privacy laws, the availability and usability of company registries, and identification mechanisms.

Legislation and sound policy to tackle threats to elections must be designed with free and apolitical expressions. Policies can potentially undermine fundamental rights such as freedom of expression. Over the past few years, many countries have either enacted or updated current cybercrime laws in an effort to address increased threats to national security. In some cases, they have produced flawed legislation that puts human rights and democracies at risk. Accused of publishing misleading information, bloggers and journalists around the world see their social media accounts closed, and in some cases, they are arrested. Transparent and unbiased mechanisms need to be in place.

3/ Promote sharing of standardised threat data and interoperability

A country can implement policies and reforms that lead to greater transparency and accuracy in the election process but that doesn't necessarily mean a rise in voter confidence. In order to be able to mitigate threats, it must be measured in a standardised way so that all stakeholders have a common understanding and can build coordinated countermeasures. Standardised

[1] .auDA (2021), .au Domain Administration Rules: Licensing, Available online: https://www.auda.org.au/policy/au-domain-administration-rules-licensing (Accessed on 14 March 2023).

data sharing regarding threats can also enable the measurement of policy effectiveness across sectors and geographies and take into consideration that one policy may protect a country's elections but might harm another country's elections simultaneously.

Practical example

The Code of Practice on Disinformation, a tool through which relevant players in the industry agreed - for the first time in 2018 - on self-regulatory standards to fight disinformation, has proven a very valuable instrument and has provided a framework for a structured dialogue between relevant stakeholders to ensure greater transparency and accountability of platforms' policies on disinformation. The Code has also prompted concrete actions and policy changes by relevant stakeholders aimed at countering disinformation. However, in order to ensure a complete and consistent application across stakeholders and Member States, the Code should be further improved in several areas by providing commonly shared definitions, clearer procedures, more precise and more comprehensive commitments, as well as transparent key performance indicators (KPIs) and appropriate monitoring. The lack of access to data allowing for an independent evaluation of emerging trends and threats posed by online disinformation, as well as the absence of meaningful KPIs, are fundamental areas for improvement of the current Code.[2]

[2] European Commission (2020), Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement, Available online: https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement (Accessed on 14 March 2023).

Technology

4/ Build cybersecurity cycles independently from election cycles

Once a technology is in place, EMBs plan closer management and monitoring of election infrastructure around voting day. Due to limited funding and resources, this process may start two to three months prior to voting day. During the roundtable discussions, elections experts related examples of election infrastructure that had been infiltrated by a malicious attacker for a year who was passively waiting for the right time to act. While every country has a different use of technology in the election process, and some countries might even have stepped back from automating the voting process, the world has more uniformly moved toward election technology to digitise voter registration and transmit and aggregate election results. As the IT attack surface grows while EMBs utilise more technology, cybersecurity resources must increase to protect that growing risk. But "cybersecurity" is often not incorporated into the IT infrastructure early enough (ideally as a requirement during system scoping), and it is not defined as a dedicated business risk by EMBs. EMBs should consider cybersecurity when making executive-level resource decisions. This can be supported with the right level of cybersecurity planning and incident response capability in-house, perhaps with a dedicated Chief Information Officer or Chief Information Security Officer, to build cybersecurity cycles that are not relying on the election cycles and remain sufficiently independent from outside ministries and agencies. In addition, the cost of cybersecurity must be adequately matched to the size of EMB IT infrastructure.

Case Study: 2014 Presidential election in Ukraine

One of the most prominent examples of an electoral cyber-attack which was shared during the roundtables and is detailed in USAID, DAI and IFES Primer: Cybersecurity and Election Paper, occurred during the 2014 presidential election in Ukraine. The attack consisted of multiple parts. Four days before the national vote, malware was planted on Ukraine's Central Election Commission (CEC) servers that rendered the vote tallying system inoperable. The system was restored using backups. On the day of the election, a distributed denial-of-service (DDoS) attack on the Ukrainian CEC shut down its website for a time. In the meantime, a Moscow TV station, broadcasted an election results website purporting to be that of the CEC that showed the election was won by a minor pro-Russian candidate. Upon seeing this, the CEC immediately began reviewing its own website and found that a fake image of inaccurate results, like the one displayed by the Moscow TV Station, had been placed on the CEC servers. If undiscovered, the image would have been displayed instead of accurate results when the polls closed at 20:00. The CEC was able to restore the correct results on its website and fix the underlying vulnerability 40 minutes ahead of the deadline.[3]

5/ Promote best practices and testing processes for each stage of the cycle

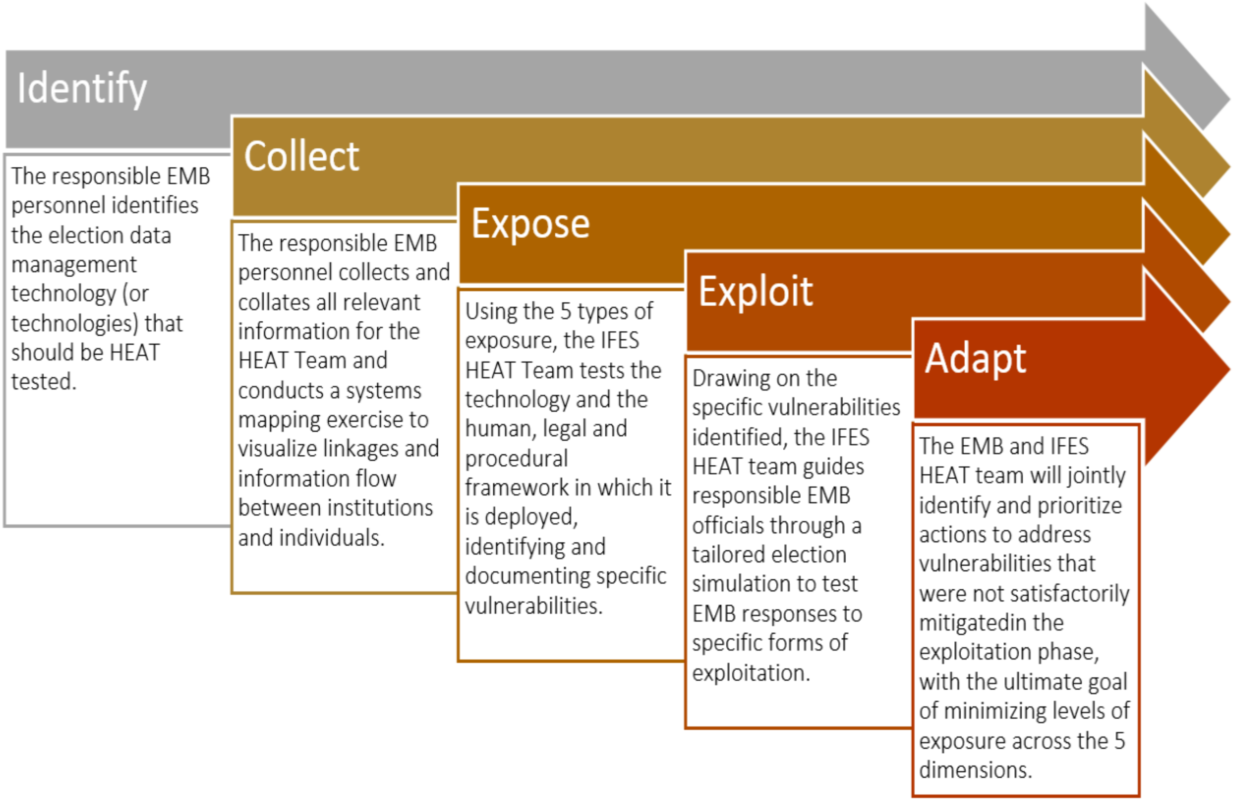
EMBs should conduct comprehensive, regular threat assessments using a tool such as the IFES HEAT[4] (Holistic Exposure and Adaptation Testing) Process. In addition to testing and audits, full election attack simulations, involving senior technical, policy-making officials, key partner agencies and, where appropriate, private sector service providers will enable the most realistic test of EMB preparedness. However, full attack simulations are expensive and time-consuming and so might be prioritised where there are significant concerns about forthcoming elections.

Existing tool: IFES HEAT Process

IFES' HEAT process - as detailed in the IFES HEAT Paper - is a process for simultaneously identifying and testing the potential exploitation of vulnerabilities in the use of election data management technology. HEAT tests the technology itself, as well as the legal and operational frameworks in which the technology is being deployed.

[3] Chaudhary, T. (2022 July), Primer: Cybersecurity and Election, USAID, DAI, and IFES publication, Available online: https://pdf.usaid.gov/pdf_docs/PA00ZK5K.pdf (Accessed on 14 March 2023).

[4] Ellena, K., Petrov, G. (2018 October), Cybersecurity in Elections: Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies. IFES, Available online: https://www.ifes.org/publications/cybersecurity-elections (Accessed on 14 March 2023).



Identify

The responsible EMB personnel identifies the election data management technology (or technologies) that should be HEAT tested.

Collect

The responsible EMB personnel collects and collates all relevant information for the HEAT Team and conducts a systems mapping exercise to visualize linkages and information flow between institutions and individuals.

Expose

Using the 5 types of exposure, the IFES HEAT Team tests the technology and the human, legal and procedural framework in which it is deployed, identifying and documenting specific vulnerabilities.

Exploit

Drawing on the specific vulnerabilities identified, the IFES HEAT team guides responsible EMB officials through a tailored election simulation to test EMB responses to specific forms of exploitation.

Adapt

The EMB and IFES HEAT team will jointly identify and prioritize actions to address vulnerabilities that were not satisfactorily mitigatedin the exploitation phase, with the ultimate goal of minimizing levels of exposure across the 5 dimensions.

Image source: Outlining the HEAT Process, IFES HEAT Paper, October 2018

Collaboration

6/ Promote transparency as a key element to trust

Transparency is a key element to trust. When transparency is missing from election technology processes it has a fundamental impact on trust. The issue of trust is an underlying component of technology development rather than a precondition. Of course, transparent use of technology cannot alone solve every trust problem, as distrust can arise from many sources. If trust was missing before the use of technology, it is unlikely that the introduction of technology would solve it. Likewise, there can be trust in the technology but not in the election process.

Greater transparency is essential to build the trust needed for a collaborative effort of all stakeholders and keeping the trust of the voters. Experts working on securing elections need to be clearly identified and not politicised. The integrity of technology is one thing, but the integrity of the people managing it is also essential to building trust in the election process. Here, the broader issue of diversity and inclusion in the sector also comes into play. These experts and policy makers need to be representative of the society. Countries should strive for transparent elections that embrace robust observation from both domestic and international observers, and international and regional standards, when existent, need to be implemented expeditiously.

Practical example

The European elections have already been subject to international election observation, but a citizen-based election observation of the European Parliament elections has not yet been conducted in a systematic manner.[5] At the time of the 2019 European elections, eight Member States had legislation and accreditation systems in place for both international and national observers. Five additional countries had respective legislation and an accreditation system for international observers but not for national observers. In Latvia, international and national election observers could be accredited without corresponding provisions in the law, while in five other member states voting, counting, and tabulation processes were fully open to the public without explicit legal provisions. The 2023 EPDE "Active citizens for a vibrant democracy" Paper shows that "only 15 (or slightly more than half) of the EU states have provisions that allow citizens to observe the procedures on election day, either by introducing the term "observers" and specifying their rights and obligations, or by more general provisions that allow all citizens to be present during voting and counting"[6].

[5] Rabitsch, A., Lidauer, M. (2019 May), Elections to the European Parliament: Needs Assessment Mission Final Report. Election-Watch-EU, Available online: https://www.wahlbeobachtung.org/wp-content/uploads/2019/02/needs-assessment-mission-report-european-elections-2019-election-watch-eu-280219.pdf (Accessed on 14 March 2023).

[6] Szyszka, S., Shlyk, A. (2023 March), Active Citizens for a Vibrant Democracy: the Role of Citizen Election Observation in the EU. EPDE, Available online:

Good practice

In Estonia, who ran Parliamentary Elections on 5 March 2023, the Election Act provides full access to citizen and international observers throughout the electoral process, including the right to observe the meetings and work of the National Election committee and election managers.[7] A coalition of civil society organisations and volunteer experts assess specific aspects of the elections and publish weekly findings that include the worst and best examples of specific candidates' compliance with the code of good conduct.

Existing initiative: the European Platform for Democratic Elections

The European Platform for Democratic Elections (EPDE) trains and supports experts and citizen election observers in EU Member States and the EU's Eastern Neighbourhood, and advocates for electoral reforms.

7/ Provide support to election management bodies to comply with high cybersecurity standards

With elections, one can't wait for the problem to be solved, you have to anticipate it and put in place high cybersecurity standards. This requires collaboration for dedicated information sharing on the threats observed and a coordinated approach to build a solution or respond to an event. Collaboration requires trust between the various stakeholders. Without trust, this process is practically impossible. Each party may be seen as a potential adversary and sharing information about vulnerabilities might expose one party or the other to more threats. This dynamic becomes more complicated as election infrastructure is further defined as critical

https://www.epde.org/en/documents.html?file=files/EPDE/RESSOURCES/2023/Study%20Citizen%20Election%20Observation/EPDE_Citizen-Election-Observation.pdf (Accessed on 27 March 2023).

[7] Rusu, A., Petrov, G. (2023 February), Estonia Parliamentary Elections: ODIHR Needs Assessment Mission Report. OSCE, ODIHR, Available online: https://www.osce.org/files/f/documents/6/5/537589.pdf (Accessed on 14 March 2023).

national infrastructure. Sometimes, instead of helping, these designations make it harder for EMBs to share information and be transparent due to the additional rules by which they need to abide. National cybersecurity agencies, in collaboration with EMBs, should consider whether the designation of election systems as part of critical national infrastructure will improve their security or add to the complexity of compliance. In both cases, National cybersecurity agencies should provide the appropriate support to EMBs to comply with these requirements.

8/ Build collaborative frameworks to help under-resourced election management bodies access information and best practices

Under-resourced EMBs often do not have robust collaboration mechanisms in place that can share information about threats, best practices, and implementable solutions to address those threats. Collaboration can begin informally. Through trust, transparency and inclusion, informal collaborations can be a significant resource for under-resourced EMBs before it turns into more robust frameworks. These can then take the shape of information sharing and analysis centres (ISACs or other, independent organisations) that provide a central resource for gathering information on cyber threats and expertise to help focus on taking positive action.

Existing Initiative: EI-ISAC

The EI-ISAC (Elections Infrastructure Information Sharing & Analysis Center) is a community of dedicated election officials and cybersecurity professionals working together to ensure the integrity of elections among U.S. State, Local, Tribal, and Territorial (SLTT) governments. It includes a 24x7x365 Security Operations Center (SOC) staffed by experienced experts to provide assistant, key support, and best practices for securing election-related systems.

Skills & Resources

9/ Promote accessible cybersecurity resources for election management bodies, media, civil society organisations, and political parties.

The lack of resources for many EMBs is a big challenge. They often don't have the budget to implement cybersecurity best practices. EMBs must work with what they have and incorporate the fact that elections are more expensive now, partly due to the increased use of technology and matching cybersecurity resources. While we hope for more resources, however, means must be found to help EMBs meet their cybersecurity challenges in the current low-resource environment. To that end, accessible - usable and affordable - cybersecurity resources must be curated for elections officials and delivered to them by mechanisms that are easy to use. This may include toolkits, joint purchasing mechanisms, shared and cloud services, and other means. In short, if election officials are facing a nail, they need a hammer or a carpenter, and not instructions on how to use a drill.

Many cyber risks lie outside the voting cycle and are targeted at government officials, campaign staff, and civil society before the election even takes place. These organisations and individuals are essential elements to the electoral cycle. However, as observed in the IFES HEAT paper,[8] EMBs or governments often focus on security concerns during the collection of data and focus less on how the data will be processed, transmitted, and stored. Means must be brought to address issues with the security of elections that lie outside the collection of data.

Elections face particular challenges when it comes to protecting systems that centralise services and/or are connected to a network. Voter registration databases are often one example of this because an attack on a voter registration database can potentially disrupt the ability to confirm a voter's eligibility when they come to vote, leading to longer wait times at a polling place (among other potential consequences). Often, some of this data can be accessed online by members of the public - either to simply check registration status or to execute voter

[8] Ellena, K., Petrov, G. (2018 October), Cybersecurity in Elections: Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies. IFES, Available online: https://www.ifes.org/publications/cybersecurity-elections (Accessed on 14 March 2023).

registration or absentee ballot requests. It can also be shared with political parties to plan their campaign. Cyber attackers may gain access to party data and subsequently release voters' personal data or release damaging information to influence the campaign. While there are cybersecurity requirements that political parties need to abide by, some smaller parties might not have the resources to be fully compliant and, therefore, require more accessible resources and training to step up their cybersecurity posture.

Existing tools and initiatives

Below is a selection of initiatives which seek to empower actors involved in elections.

	Global	Europe	Asia
EMBs	GCA Cybersecurity Toolkit for Elections The toolkit provides election officials with free and effective tools to implement the best practices in the EI-ISAC's Essential Guide to Election Security. IFES social media Tools for Election Management Suite of tools to aid EMBs disseminate credible information in ways that reach new audiences, build visibility, and trust, and enable voters to engage directly with election authorities.	Council of Europe Electoral training centres established in the Republic of Moldova, Georgia and Bosnia and Herzegovina to provide standardised, quality instruction to election officials.	
SCOs	IFES Inclusive Digital Advocacy Toolkit and Chain of Harm Methodology The toolkit is a resource to support CSOs to use social media and technology in advocacy activities. The Chain of Harm Methodology is a tool for online false information and dangerous speech research. NDI Cybersecurity Handbook for Civil Society Organizations The Handbook is a guide for civil society organisations looking to get started on a cybersecurity plan. NDI also has a Learning Portal for organisations.		Asian Network for Free Elections (ANFREL) produced a number of election observation handbooks and toolkits to support civil society groups, media, and other relevant actors in Asia. They accompany these with capacity building workshops.

Media	GCA Cybersecurity Toolkit for Journalists The toolkit provides independent journalists, watchdogs, and small newsrooms free and effective tools to reduce cyber risk.		
Political Parties	NDI Cybersecurity Handbook for Political Parties The Handbook is an open-source resource designed to help political parties develop an understandable and implementable cybersecurity plan. NDI also has an interactive game designed to teach best practices to those active in campaigns. IRI Political Parties Playbook: A Guide for Digitizing Party Operations This playbook helps political parties of all capacity levels take steps to expand their operations online and increase their overall capacity to operate digitally.	Harvard Belfer Center, NDI and IRI Cybersecurity Campaign Playbook: European Edition This playbook is designed for the European election landscape and gives simple, actionable information to make campaign's information more secure for any political party. U.K. NCSC Guidances for political parties and individuals in politics These guidelines have been produced by the United Kingdom NCSC. One is for political parties and provides information about common cyber-attacks and preventative measures. The other one is for individuals in politics, including elected representatives, candidates, and activists.	Harvard Belfer Center, NDI and IRI Cybersecurity Campaign Playbook: India Edition This playbook is designed for the Indian election landscape and gives simple, actionable information to make campaign's information more secure for any political party.

10/ Promote digital skills and literacy - including cybersecurity - programmes

Threats to the integrity of elections include malinformation campaigns, and the proliferation of malinformation was a top concern among the UK and Western European roundtable participants. Private companies and social media platforms also acknowledge that fake accounts are a threat to the integrity of elections. Since 2016, participants observed a rise of malinformation which escalated with COVID-19, the storming of the Reichstag in August 2020, the U.S. Capitol attack on 6 January 2022, the War in Ukraine, and the Brazil Congress riot on 8 January 2023. Malinformation and propaganda is an old problem, but the cyber dimension gives the propagandist new tools. The novelty lies above all in the viral nature of this information, true or false, relayed on social networks and discussion forums and in the multiplication of dissemination methods and actors. In this context, election officials, political parties, and the media are more vulnerable than the election activities themselves. Adversaries use cyber capabilities to publicly discredit individuals or the election process as a whole, spread disinformation and propaganda, and shape the opinions of voters. Sometimes, one small-scale intrusion, or the perception of an intrusion, can have an outsized impact. With perception hacking, elections can be fairly secure and the process fine but one mistake - or accusation of mistake - can trigger a spiral of mistrust. Individuals involved in the elections need to be empowered with the right set of skills based on a recognised skills framework to handle things with caution when responding to these incidents.

Internationally used digital skills frameworks

There are several digital skills frameworks used around the globe. While some of these are used internationally, some are specifically curated to meet the needs of specific countries. Below is a selection of internationally used digital skills frameworks.

Global	Europe	United Kingdom
The DQ Framework The framework, formed in 2018 by the OECD, IEEE SA, and DQ Institute in association with the World Economic Forum, represents critical skills needed to thrive in the digital age and aggregates more than 25 prior leading frameworks globally to lay out a common language, structure, and taxonomy about digital literacy.	The European Digital Competence Framework for Citizens (DigComp) The framework identifies 21 competences in five key areas, describing what it means to be digitally savvy. These are: 1. Information and Data Literacy 2. Communication and Collaboration 3. Digital Content Creation 4. Safety 5. Problem Solving	The Essential digital skills framework This framework sets out five categories of essential digital skills for life and work to support training for adults. These are: 1. Communicating 2. Handling information and content 3. Transacting 4. Problem solving 5. Being safe and legal online

At the voter level, one needs to be able to identify “clean” information to make an informed decision. Media and digital literacy is key to better equip generations as they grow. In addition, the field of cybersecurity and the election processes need to be demystified and democratised. There’s a need to raise awareness on what cybersecurity is and what secure elections are and are not, and to raise citizen’s awareness of online malinformation and propaganda practices.

Existing tools and initiatives

Below is a selection of initiatives which seek to empower citizens.

	Global	Europe
Awareness	AI Forensics builds free software tools for algorithmic analysis and is involved in social media monitoring for election integrity. Digital Forensic Research Lab, an initiative of the Atlantic Council aiming to identify, expose, and explain disinformation using open-source research.	IRI’s Beacon Project has been monitoring media presence in the context of elections and provides analysis and accessible, user-friendly, data since 2015.
Training	The Media Manipulation Casebook is a digital research platform intended to support the detecting, documenting, describing, and debunking of misinformation, disinformation, and media manipulation. DROG offers workshops and educational programmes and creates innovative interventions that help citizens build resistance to disinformation in a non-traditional way. Its subsidiary Bad News is an award-winning disinformation game exposing the tactics and manipulation techniques that are used to mislead people.	Lie Detectors is a non-profit, award-winning media literacy organisation that works to empower school children and teachers in Europe to tackle fake news and make informed choices. It offers training sessions in classroom settings and teacher-training events free of charge.
Collaboration	DISARM is an open-source framework for fighting disinformation through sharing data, analysis, and coordinating effective actions.	EU DisinfoLab develops and maintains an independent European platform on disinformation, providing experts with tools and resources to encourage collaboration.

About the Global Cyber Alliance

The Global Cyber Alliance (GCA) is an international, cross-sector effort dedicated to eradicating cyber risk and improving our connected world. GCA works with a partner community worldwide to build practical, accessible resources and measure their impact, in order to achieve a secure, trustworthy Internet that enables social and economic progress for all. Learn more at www.globalcyberalliance.org.

New York
731 Lexington Avenue
New York, NY
10022
UNITED STATES

London
City of London Police
3rd Floor
Guildhall Yard East
London
EC2V 5AE
UNITED KINGDOM

Brussels
Scotland House
City Office in Brussels
(c/o Global Cyber Alliance)
Rond Point Schuman 6
1040 Brussels
BELGIUM

Contact the lead author
Ms. Kayle Giroud
kgiroud@globalcyberalliance.org

GLOBAL
CYBER
ALLIANCE™