GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

PROTECTING THE ELECTORAL PROCESS AND ITS INSTITUTIONS

Sean Kanuck
Director for Future Conflict & Cyber Security
The International Institute for Strategic Studies

GCSC **THOUGHT PIECE**
JANUARY 2018

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

PROMOTING STABILITY IN CYBERSPACE TO BUILD PEACE AND PROSPERITY

The Global Commission on the Stability of Cyberspace (GCSC) engages the full range of stakeholders to develop proposals for norms and policies that enhance international security and stability and guide responsible state and non-state behavior in cyberspace.

🐦 @theGCSC
www.cyberstability.org
info@cyberstability.org
cyber@hcss.nl

The GCSC does not specifically endorse the respective publications, nor does it necessarily ascribe to the findings or conclusions. All comments on the content of the publications should be directed to the respective authors.

The opinions expressed in this publication are solely those of the author and do not reflect the views of the Global Commission on the Stability of Cyberspace (GCSC), its partners, or *The Hague* Centre for Strategic Studies.

The Hague Centre for Strategic Studies

Lange Voorhout 1
2514 EA The Hague
The Netherlands

info@hcss.nl
HCSS.NL

EastWest Institute (EWI)

www.eastwest.ngo
communications@eastwest.ngo

ABOUT THE GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE

The Global Commission on the Stability of Cyberspace (GCSC) helps to develop norms and policies that advance the international security and stability of cyberspace. It promotes mutual awareness and understanding among the various cyberspace communities working on issues related to international cybersecurity. By finding ways to link the various intergovernmental dialogues on international security with the new communities created by cyberspace, the GCSC fulfils a critical need: supporting policy and norms coherence related to the security and stability in and of cyberspace by applying a multi-stakeholder approach to its deliberations on peace and security.

Chaired by Marina Kaljurand, and Co-Chaired by Michael Chertoff and Latha Reddy, the Commission comprises 26 prominent Commissioners representing a wide range of geographic regions as well as government, industry, technical and civil society stakeholders with legitimacy to speak on different aspects of cyberspace.

The GCSC Secretariat is provided by The Hague Centre for Strategic Studies and supported by the EastWest Institute.

ABOUT THE AUTHOR

Sean Kanuck is an international attorney and strategic consultant who advises governments, corporations, and entrepreneurs on the future of information technology. Sean serves as Director of the Future Conflict and Cyber Security program at the International Institute for Strategic Studies (London, UK) and Chair of the Research Advisory Group for the Global Commission on the Stability of Cyberspace (The Hague, Netherlands). He has also been appointed as a Distinguished Visiting Fellow at Nanyang Technological University (Singapore), a Distinguished Fellow with the Observer Research Foundation (New Delhi, India), and an Affiliate with Stanford University's Center for International Security and Cooperation (Palo Alto, USA).

Sean served as the United States' first National Intelligence Officer for Cyber Issues from 2011 to 2016. He came to the National Intelligence Council after a decade of experience with the Central Intelligence Agency's Information Operations Center, the White House National Security Council, and the United States delegation to the United Nations Group of Governmental Experts on international information security. Prior to government service, Sean practiced law with Skadden Arps in New York, where he specialized in mergers and acquisitions, corporate finance, and banking matters. He holds degrees from Harvard University (A.B., J.D.), the London School of Economics (M.Sc.), and the University of Oslo (LL.M.). He also proudly serves as a Trustee of the Center for Excellence in Education in McLean, Virginia.

PROTECTING THE ELECTORAL PROCESS AND ITS INSTITUTIONS

Sean Kanuck
Director for Future Conflict & Cyber Security
The International Institute for Strategic Studies

GCSC **THOUGHT PIECE**
JANUARY 2018

PURPOSE

This thought piece is prepared for the Global Commission on the Stability of Cyberspace (GCSC) to (a) facilitate its understanding of critical cyber security issues related to protecting the democratic institutions necessary to conduct free and fair elections, and (b) identify key topics that may be suitable for further research commissioned by the GCSC.

SCOPE

In keeping with the intent of the GCSC commissioners and the draft Request for Proposals (RFP) on this topic, this thought piece limits its discussion to the actual mechanisms of conducting elections and does not address foreign or domestic influence campaigns aimed at manipulating an electorate's preferences. Those issues have been analyzed elsewhere by this author[1] and merit further attention; however, they lie outside the scope of this paper.

OVERVIEW

In order to answer the key research question "How can the mechanics of democratic institutions and electoral processes be protected from disruption and fraud by cyber (or cyber-enabled) operations?", one must examine the full "life cycle" of the electoral process. That includes the proper identification and registration of voters, advance notification of upcoming elections and candidates, verification of voters on election day, casting of ballots, tabulation and certification of votes, and audit procedures after the election. The overarching democratic principles involved are (1) equality and (2) integrity. The first strives to ensure that each qualified citizen receives the right to cast one, and only one, vote in an election. The second strives to ensure that the vote of each citizen is properly recorded and represented in the aggregate results that are officially recognized. Most of the institutions and activities in that overall process are directly managed by government authorities; however, they rely on commercially manufactured information technology products as well as other public infrastructures (such as electric and telecommunications utilities). The following analysis will consider each phase of the electoral process to expose its potential vulnerabilities.

IDENTITY

Discussion about democratic elections must necessarily start with the "demos", or the people themselves. Before one can assess if votes are properly cast or properly recorded, one must know who is eligible to cast ballots … and even more fundamentally, who is who. In today's world of biometrics and cryptographic hashes, it is simply unacceptable for ballots to be cast in the name of dead persons or for the same individual to cast multiple ballots. Moreover, it is equally unacceptable that many people on the planet still have no verifiable identity or proof of their existence. Not only does that enable human trafficking and other injustices, but it also precludes them from participating in democratic governance. Identity is actually the ultimate foundational requirement of democratic elections. The Unique Identity Authority of India, also known as "Aadhaar", represents a large-scale effort to create verifiable, biometric identities for the citizens

[1] See e.g., Sean Kanuck, "Hacking Democracy" in Digital Debates CyFy Journal, Volume 4 (2017), available at: http://cf.orfonline.org/wp-content/uploads/2017/10/CyFy_2017_Journal.pdf; see also, Sean Kanuck, "Get ready for Democracy 3.0" in The Hill, 25 October 2017, available at: http://thehill.com/opinion/cybersecurity/356965-get-ready-for-democracy-30.

of that country.[2] Countries, such as the United States, whose political culture opposes even a national identity card will face challenges to eradicating voter fraud based on uncertainties regarding identity and the status of potential voters. But even countries with strong identity systems will still face cyber security threats to the integrity and availability of those databases. The physical interface only occurs upon initial sampling and then periodic scanning; the real implementation involves the digitally stored information that must be queried from time to time. All biological identity intelligence issues actually get reduced to information security issues since analogue records are not used for either "1-to-1" matching (i.e., positive identification) or "1-to-N" searches (e.g., to permit access to documented persons or to prohibit access to watch-listed persons).[3] Compromised software algorithms could theoretically approve or disapprove persons inconsistent with data records, or records could be illegitimately added to or deleted from such databases.

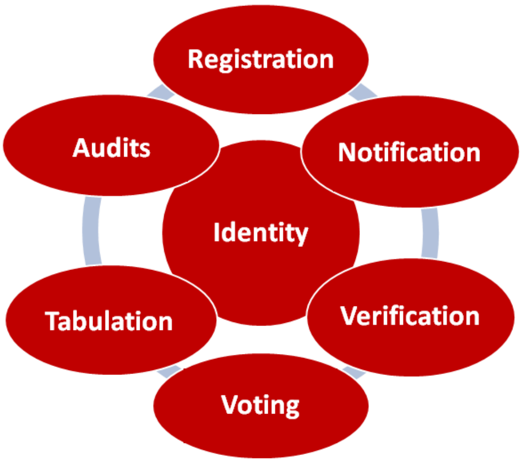

FIGURE 1: "LIFE CYCLE" OF THE DEMOCRATIC ELECTION PROCESS

REGISTRATION

Voter registration represents the first formal part of the election process. Identity is used to certify individuals' right to vote and they are placed on an approved voter list. This paper will not address procedural or physical measures used to discriminate against qualified voters in many jurisdictions and prevent them from being able to cast a ballot on election day. Instead, it will simply acknowledge that voter registration information is ubiquitously stored in computer databases today (even when printed lists are created for polling stations on the day of specific elections), thereby making those voter registries susceptible to the same hardware, software, supply chain, physical access, insider threat, and other cyber security concerns that make every information technology system vulnerable to exploitation.

[2] See https://uidai.gov.in/.

[3] See generally, Office of the Director of National Intelligence, National Intelligence Council Report (NICR 2014-06), "Identity Technologies: Trends, Drivers, and Challenges: An Industry Discussion", 13 August 2014, available at: https://www.dni.gov/files/documents/NICR_2014_06Identity_Technologies_FINAL.pdf.

NOTIFICATION

Government authorities must be able to accurately inform prospective voters of when and where elections will take place. That means that governments must have secure and reliable methods for broadcast communications, and that voters must know not to believe unofficial information from other sources. For example, in Canada's 2011 federal election, one political party conducted "robocalls" to misinform voters from the opposing party that the polling locations had been changed.[4] Such illicit efforts underscore the need for reliable online information sources that cannot be compromised or manipulated. Once again, that means election notification systems are also susceptible to the same hardware, software, supply chain, physical access, insider threat, and other cyber security concerns that make every information technology system vulnerable to exploitation.

VERIFICATION

On election day, voters who physically present themselves at the polling station must have their identities verified. In a biometric confirmation context, the cyber threat considerations discussed in the "Identity" section above would apply. In an identity card confirmation context, then the technological security measures used in producing those identification cards will be determinative. The integrity of democratic elections then becomes dependent on the information security of many networks unrelated to the election systems (e.g., the systems that generate passports, driver licenses, etc.) and the physical anti-fraud features of the identification cards themselves (e.g., special polycarbonate materials, embedded holograms, etc.). Positive government control of the production capacity for those security features also likely rests on the cyber security of multiple computer systems.

VOTING INFRASTRUCTURE

The actual procedures and equipment used for voting represent another vector for cyber threats to compromise elections. The moment machines are introduced to optically scan and record paper ballots, votes are cast on electronic machines ("e-voting"), or elections are conducted online over the Internet ("i-voting"), then the integrity of the results can be affected by cyber attacks. Much technical research has already been done on this topic, and the US Congress has also held specialized hearings on the issue in recent years.[5] This paper will not try to detail all of the technical vulnerabilities associated with various voting machines; readers are instead referred to the sources in the footnotes. Suffice it to say, though, that basically every voting machine that has been rigorously tested has been penetrated. For example, a Harvard study has reported *inter alia* that auditors in Virginia were able to crack weak password settings of voting machines with wireless connections and that supply chain limitations on key parts could even

[4] See http://news.nationalpost.com/news/canada/canadian-politics/electoral-fraud-didtake-place-in-2011-federal-vote-but-it-didnt-affect-outcome-judge-rules.

[5] U.S. House of Representatives, Committee on Science, Space, and Technology, "Full Committee Hearing - Protecting the 2016 Elections from Cyber and Voting Machine Attacks", 13 September 2016, available at: https://science.house.gov/legislation/hearings/full-committee-hearing-protecting-2016-elections-cyber-and-voting-machine; and U.S. House of Representatives, Committee on Oversight and Government Reform, Subcommittees on Information Technology and Intergovernmental Affairs, "Cybersecurity of Voting Machines", 29 November 2017, available at: https://oversight.house.gov/hearing/cybersecurity-voting-machines/.

obstruct regular voting.[6] In regard to optical scanners and direct electronic recording (DRE) machines, J. Alex Halderman from the University of Michigan has testified that, "Fundamentally, they suffer from security weaknesses similar to those of other computer devices. I know because I've developed ways to attack many of them myself as part of my research into election security threats."[7] In 2017, the DEFCON 25 conference hosted a "hacking village" to examine voting equipment and achieved similar success in identifying vulnerabilities that are detailed in a DEFCON report.[8] The risks and potential rewards of i-voting have also been examined in detail.[9] Of course, i-voting over personal computers or mobile devices is fully reliant on the confidentiality, availability, and integrity of those de-centralized, commercial platforms as well as the computer networks managed by the government authorities conducting the election. So once again, that means i-voting infrastructure is also susceptible to the same hardware, software, supply chain, physical access, insider threat, and other cyber security concerns that make every information technology system vulnerable to exploitation.

TABULATION

When it comes to tabulating election results, one must have two considerations: (1) whether all of the votes that were cast and recorded are aggregated accurately; and (2) whether all of the eligible votes that were supposed to be cast (and which the respective voters believed were cast) were indeed recorded correctly. In regard to the second issue, one must concede that interference with or disruptions of public utilities (such as electricity or telecommunications) could adversely impact e-voting and i-voting by preventing certain votes from being cast. A significant disruption would warrant a re-vote to ensure legitimacy; however, one can easily imagine a scenario where localized Internet impediments disadvantaged certain voters but judicial oversight would not mandate a re-vote. The real issue becomes whether – or how – a voter would even know if their e-vote or i-vote was actually transmitted and properly recorded. That would be especially difficult if the hackers conducted a man-in-the-middle attack and returned a spoofed confirmation message: a voter may never know that they had not connected to the actual voting sight. Such sophisticated cyber attacks would no-doubt need to either defeat or circumvent cryptographic safeguards, but such successes have occurred even where the stakes were much lower than a national election. Returning to the first issue, the aggregation of votes requires machines to report their own totals and to communicate them to other machines or persons (who then enter them into other machines). Malicious software could be written to make those machines "state aware" and to respond differently under different

[6] Ben Buchanan and Michael Sulmeyer, Harvard Kennedy School, Belfer Center Cyber Security Project, "Hacking Chads: The Motivations, Threats, and Effects of Electoral Insecurity", October 2016, available at: https://www.belfercenter.org/sites/default/files/files/publication/hacking-chads.pdf.

[7] J. Alex Halderman, Expert Testimony before the U.S. Senate Select Committee on Intelligence, 21 June 2017, available at: https://www.intelligence.senate.gov/sites/default/files/documents/os-ahalderman-062117.pdf.

[8] Matt Blaze, Jack Braun, Harri Hursti, Joseph Lorenzo Hall, Margaret MacAlpine, and Jeff Moss, *DEFCON 25 Voting Machine Hacking Village, "Cyber Vulnerabilities in US Election Equipment, Databases, and Infrastructure*", September 2017, available at: https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf.

[9] Peter Haynes and Jason Healey, Atlantic Council, "Online Voting: Rewards and Risks", 2014, available at: https://www.verifiedvoting.org/wp-content/uploads/2014/10/Online_Voting_Rewards_and_Risks.pdf.

circumstances (e.g., during a partial audit and an actual full election). This would be analogous to the methodological approach that Volkswagen used to defraud emissions testing from 2008 to 2015.[10]

AUDITS

Therefore, the ability to audit election results becomes the only ultimate safeguard for protecting democratic elections. In most e-voting and i-voting contexts, there is no means for a voter to independently check and verify that their vote was recorded properly – let alone aggregated properly. It is of course possible to introduce such capabilities through technical means. Alex Halderman argues for always having a paper ballot to refer back to and maintains that "we need to consistently and routinely check that our election results are accurate, by inspecting enough of the paper ballots to tell whether the computer results are right."[11] As with any other critical infrastructure, the resiliency of the election/voting infrastructure consists of strong defenses to prevent compromises as well as intentional redundancy to overcome any compromises or occasional degradations.

POLITICAL CONSIDERATIONS

It is worth noting that improved security and fidelity will almost always come with a cost, either in money or time. Each polity will need to strike a balance between how many resources it can reasonably afford to spend on its elections versus other political priorities. In the end, probably no measure of cyber security will be able to protect against genuine insider threats – especially if they come from individuals empowered by a ruling administration to alter election results. Institutional transparency and the active involvement of observers from the opposition is fundamental to protecting democratic elections.

PHILOSOPHICAL CONSIDERATIONS

The issue of independent verification raises questions about the future of the secret ballot. Would modern voters prefer to conceal their political preferences or be certain that their voice was heard? Moreover, is it technologically feasible for them to have their cake and eat it too? (And that means not just an encrypted correspondence with a government computer returning the same voting data that it received from the user; but rather, a genuine ability to track one's input – and everyone else's – all the way through the aggregation process, such as a blockchain could provide.) One final query is paramount to the overall topic of protecting any democracy that relies on public confidence, namely "What level of uncertainty in election results is acceptable to still maintain legitimacy?" Audits can only provide statistical certainty within prescribed margins of error. What is the acceptable level of statistical uncertainty that can be ignored?

[10] See http://www.bbc.com/news/business-34324772.

[11] Supra note 8.

RECOMMENDATIONS

Voting is the essential “transaction” of democracy and the integrity of that process needs to be protected as much if not more than any other financial or economic transaction. Towards that end, ten recommendations for safeguarding electoral systems are offered below. Recommendations (1) through (4) involve improving the defenses of existing voting systems. Recommendations (5) and (6) speak to developing better systems for the future. Finally, recommendations (7) through (10) are intended to provide an *ex post* “check sum” on the system to guarantee its results are valid.

(1) Subject all electronic voting machine hardware and software to rigorous “red teaming” (i.e. penetration testing) by offensive experts from the government and private sector.

(2) Harden voting machines against all electromagnetic transmissions.

(3) Conduct tests of electronic voting machines with sample sizes equal to election-day turnouts and on the same calendar date (i.e. internal clock setting) as the election itself.

(4) Properly vet all polling station personnel who will have physical access to voting machines. (This also applies to access to any storage facilities between elections.)

(5) Predicate any future online or wireless voting capabilities upon biometric verification.

(6) Fund research and development of advanced technologies (e.g. blockchain, quantum cryptography, etc.) for establishing secure, online elections in the future.

(7) Maintain all original paper ballots indefinitely for audit purposes.

(8) Conduct random audits of paper ballots to verify electronic vote tallies as well as mandatory audits of paper ballots for precinct results within a specified margin of error.

(9) Provide an opt-in capability for voters to verify if their own votes were recorded accurately. (Many voters may prefer this option to an uncertain secret ballot.)

(10) Apply machine learning algorithms to detect statistical anomalies for further investigation (cf. insider trading and credit card or telecommunications billing fraud.)

SECRETARIAT

The Hague Centre for Strategic Studies

EastWest INSTITUTE

PARTNERS

Ministry of Foreign Affairs

CSA SINGAPORE

Microsoft

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE
DE L'EUROPE ET DES
AFFAIRES ÉTRANGÈRES

Internet Society

SPONSORS

Ministry of Foreign Affairs
Of Estonia

SUPPORTERS

Black Hat USA
Packet Clearing House