United Nations Office of Drugs and Crime

Middle School
Sept 2018

Original: English

United Nations Office of Drugs and Crime:

The Commission of Crime Prevention and Criminal Justice

Committee History

United Nations Office of Drugs and Crime (UNODC) is a global leader in the fight against illicit drugs and international crime. Established in 1997 through a merger between the United Nations Drug Control Programme and the Centre for International Crime Prevention, UNODC operates in all regions of the world through an extensive network of field offices. UNODC relies on voluntary contributions, mainly from Governments, for 90 per cent of its budget.

The Commission acts as the governing body of the United Nations Office on Drugs and Crime. It approves the budget of the United Nations Crime Prevention and Criminal Fund, which provides resources for promoting technical assistance in the field of crime prevention and criminal justice worldwide.

The Commission on Crime Prevention and Criminal Justice (CCPCJ) is part of the Economic and Social Council (ECOSOC). It focuses on transnational crime and criminal justice. In the early 1990s, the UN developed a greater interest in criminal justice policy, which led to the creation of the CCPCJ. When the CCPCJ was created, a similar older committee (called the Committee on Crime Prevention and Control) was removed. This was done in order to put more focus on the CCPCJ and make sure that UN agencies would coordinate well with each other.

Addressing Cybercrime to Protect Election Legitimacy

History

As technology progresses and new electronic election methods are created, the challenge of cybercrime needs to be addressed in order to protect election legitimacy. The CCPCJ is committed to upholding the ideals in Article 21 of the United Nations Declaration of Human Rights (UDHR):

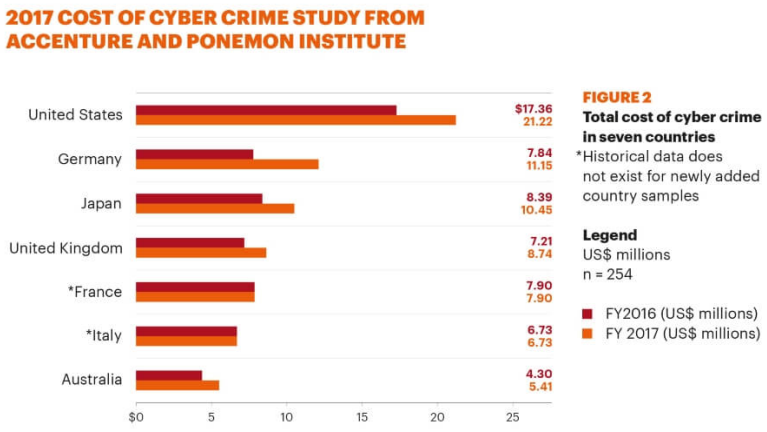
> *(1) Everyone has the right to take part in the government of his country, directly or through freely chosen representatives;*
> *(2) Everyone has the right of equal access to public service in his country;*
> *(3) The will of the people shall be the basis of the authority of government; this will shall be*

expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures.

The mandate of the CCPCJ allows it to address the use of technology in fair elections. Thus, it is not only the responsibility of national government, but also the responsibility of the international community to help ensure fair elections.

Online voting, while currently not a widespread practice, gives voters an opportunity to voice their opinion when otherwise not possible. First introduced in the United States in 2000, online voting has spread to fourteen other countries. Canada, France, and Switzerland currently offer online voting to all citizens. Online voting excels in its accessibility: it allows people to vote when they otherwise would not be able to do so. Transportation, health, or geographical reasons are just a few examples of issues that might prevent someone from voting in the absence of an online option.

However, despite all the benefits of online voting, there are concerns about its security. Worried by rigged elections and hackers, many people are concerned about the truth of online voting. Public trust in governments to prevent hacking has been shaken by high profile hacks on political parties. An example is when the Democratic Party of the United States had its emails hacked and released online in 2016. Technical institutions and experts can help to improve security, often breaking down the 'black boxes' that are online voting. There are many technologies in place to help prevent online hacking, such as HTTPS, unique identifier (UID), and anti-spam technologies.



Different countries take very different approaches to the electronic security of their elections. While many countries have not wanted to rely too heavily on technology for elections, the Republic of Estonia has enthusiastically developed an extensive e-government platform. This allows citizens to manage their votes and most of their government interactions online, rather than having to visit different government offices. In 2007, Estonia became the first country in the world to use an online voting system for a national election. Despite Estonia's advocacy, other countries have not been so quick to adopt new technologies. Many still worry about how safe these voting methods are, and this ear has caused some countries to even reduce the technology in their voting process. The way in which states handle cybercrime is linked to the type of crime they are dealing with. With this, delegates and the countries they represent are tasked with finding individual solutions to a collective problem.

Recent Developments

Despite all the developments in voting technologies, many countries have been slow to adopt them, even the more economically developed countries in the world like the United States. Recent challenges have undermined faith in electronic voting methods and have caused some to call for a return to paper voting systems. For example, in the United States, a precinct in northeastern Georgia reported a 247% voter turnout. When investigators wanted to audit this result, the backups of the voting systems were destroyed.

On the other hand, economically developing countries have seen tremendous growth in adopting electronic voting systems. Mexico, once a one-party state, has been able to make changes. After a major

election controversy in 1998, Mexico instituted an independent electoral body to oversee election policies. Mexico has since adopted an electronic voting system in conjunction with a paper system to ensure that if either system fails, there will be a backup record. The Independent Electoral and Boundaries Commission of Kenya (IEBC) has recently announced its plans to implement blockchain technologies in its elections to improve voter trust and transparency. Blockchain technologies work such that each new entry is dependent on the previous entry's hash (or unique identifier), making it very hard to fake an entry or change existing entries. However, these methods are more challenging to implement than standard electronic voting methods.

Treaties and Agreements

Because electronic election hacking is relatively new, there are fewer international treaties on how the global community should address it. The Convention on Cybercrime, signed in 2001, was an early attempt to provide standards around lawful online activity between organizations and countries. The treaty deals with a wide range of cybercrime, such as fraud, copyright violations, etc. While the treaty does require countries to outlaw hacking, it makes no specific mention of voting systems. Another challenge limiting the usefulness of the Convention on Cybercrime is the fact that only 57 countries have ratified it, the majority of which are in Europe. Many important countries such as Brazil, Russia, India, and China have not ratified the treaty, and therefore the treaty lacks global force.

In fact, the lack of international treaties surrounding election hacking has caused some to wonder whether countries have any legal protection from hacking at all. Many legal scholars have argued that the protection against the "use of force" guaranteed by the United Nations Charter does not apply to electronic hacking and only applies to physical force. This means that the current framework for addressing these issues is very informal, relying on the good will of the countries involved to prevent further attacks.

Guiding Questions

- How widespread is the use of computers and similar technology in your country?
- What percentage of your population has regular internet access?
- What type of election system does your country use? Does it rely on paper voting systems, electronic voting systems, or a combination of the two?
- Has your country been subject to any recent election scandals regarding the use of technology?
- Does your country offer online voting? If so, are there any security measures currently in place to protect the system from being hacked?
- Has your country ever been targeted in a cyber-attack from a foreign country? If so, how has your country dealt with it?

BIBLIOGRAPHY

"Chapter I." United Nations. Accessed 15 July 2018. http://www.un.org/en/sections/un-charter/chapter-i/index.html.

Text of the UN Charter.

Council of Europe. "Budapest Convention and Related Standards." Cybercrime. Accessed August 24, 2018. https://www.coe.int/en/web/cybercrime/the-budapest-convention.

This is the Council of Europe's page regarding the Convention on Cybercrime, including the treaty text and other related documents.

"Election Monitoring: An Early Warning Perspective and Governance Capacity Building Strategy." *United Nations*. Last Modified 28 September 2001. http://unpan1.un.org/intradoc/groups/public/documents/CAFRAD/UNPAN005424.pdf.

This article outlines electronic elections and electoral administration via workshop format in Africa.

Rodriguez, Andrea. “Ahead of Mexico's presidential election, fears and warnings over possible fraud.” *Chicago Tribune*. Last Modified 29 June 2018. http://www.chicagotribune.com/news/nationworld/ct-mexico-election-fraud-warning-20180629-story.html

This article from the Chicago Tribune highlights the election fraud of Mexico’s past

Condon Christine, “Bizarre tales, confusing ballots from Georgia’s primary contained in federal lawsuit.” *McClatchy DC Bureau.* Last Modified 6 August 2018. https://www.mcclatchydc.com/latest-news/article216056560.html.

This article details the Georgia election fraud.

Hundeyin, David. “Kenya’s Electoral Commission to Adopt Blockchain for Enhanced Vote Integrity.” *CNN*. Last Modified 23 August 2018. https://www.ccn.com/kenyas-electoral-commission-to-adopt-blockchain-for-enhanced-vote-integrity/.

This article discusses the implementation of blockchain in and history of Kenyan elections.

Sachs, Ram. “Yale Journal of International Law | Hacking the Election.” Yale Journal of International Law, October 28, 2016. http://www.yjil.yale.edu/hacking-the-election/.

This is a legal article that discusses how the UN is poorly equipped to address cybercrime and hacking.