

Exercise Background Material

Rwanda

Country Profile



Points of Contact: Rebecca Beigel, Julia Schuetze | Stiftung Neue Verantwortung e. V.
Beisheim Center | Berliner Freiheit 2 | 10785 Berlin



Disclaimer:

The research only represents a country's cybersecurity policy to a limited extent and is not an in-depth or complete analysis or assessment of current policy. In order to adapt the exercises to specific countries, it is important to understand the broader strokes of cybersecurity policies of other countries. Our team, therefore, researches publicly available information on cybersecurity policies of countries to adapt the exercises to country-specific needs. The research is shared with participants as background material in preparation for the exercise. Therefore, the documents have a timestamp and consider policy up until the date of publication. In the interests of non-profitability, we decided to make the background research publicly available. If you are using these materials, please include the disclaimer. Please also do not hesitate to contact us.

Endnotes marked with an asterisk (*) mean that the respective website link is currently not available. The websites were last accessed 31st of January, 2021. The original version of this country profile was published in July 2021.

This material is licensed under CC BY SA 4.0

Points of Contact:

Rebecca Beigel

Project Manager for International Cybersecurity Policy

rbeigel@stiftung-nv.de

+49 (0)30 40 36 76 98 3

Julia Schuetze

Junior Project Director for International Cybersecurity Policy

jschuetze@stiftung-nv.de

+49 (0)30 81 45 03 78 82



Table of Contents

Political System and Socio-Political Background

Key Facts

Political System

Socio-Political Context

Rwanda's Cybersecurity Policy

Vulnerability and Threat Landscape

Key Documents

Legal Framework

Cybersecurity Architecture - Selected Institutions

Bilateral and Multilateral Cooperation



Political System and Socio-Political Background

Key Facts

- Official country name: the Republic of Rwanda¹, Kigali is the capital²; Population: densely packed population of about 12.6 million people (2019)³; Official languages: Kinyarwanda, French, English, and Swahili⁴;
- Currency: Rwandan franc⁵.

Political System

- Form of Government: Presidential Republic⁶;
- Head of State: Paul Kagame, President of Rwanda, inaugurated April 22, 2000, Rwandan Patriotic Front (RPF)⁷;
 - Head of State and Commander-in-Chief of the Armed Forces;
 - Nominates the Prime Minister and appoints the Council of Ministers;
- Head of Government: Edouard Ngirente, inaugurated August 30, 2017⁸;
- Bicameral Legislature: Chamber of Deputies and Senate⁹.

Socio-Political Context

Rwanda's leadership focuses on economic reconstruction and development¹⁰:

- Aims to reach Middle Income Country (MIC) status by 2035¹¹;
- Rwanda now follows a series of seven-year National Strategies for Transformation after implementing Economic Development and Poverty Reduction Strategies;
- The National Strategies for Transformation includes priority areas focusing on skill development in cybersecurity and enhancing regional and international partnerships to fight cybercrime, amongst others¹².

Part of Rwanda's economic development is the enhancement of its digital infrastructure and development, with visible success:

- Over the past five years, Rwanda's access to international bandwidth has grown ten-fold¹³;



- The mobile network coverage has also increased: 3G network coverage is now at 93.5 percent, compared with a regional average of 76 percent¹⁴;
- Rwanda's internet penetration rate reached 52.1 percent in 2018¹⁵.

COVID 19-pandemic has disrupted Rwanda's economic growth, which was thriving in 2019. Amongst other sectors, the pandemic hit exports, international trade, and the tourism sector¹⁶.

Freedom of opinion, media, association, and expression are severely restricted in Rwanda¹⁷; Rwanda ranked 155 on the 2020 World Press Freedom Index¹⁸.



Rwanda's Cybersecurity Policy

Vulnerability and Threat Landscape

A study by a UK Cyber Security and Threat Intelligence firm found that the majority of Rwandan firms are vulnerable to cyber threats. Only 26 out of 750 firm systems were reviewed as good; the largest vulnerabilities were found through email scams (e.g., phishing)¹⁹. The rate of cybercrimes increased by 72% during the first COVID-related lockdown between January and March 2020. Mobile money frauds were particularly popular during the lockdown, according to the Rwanda Investigation Bureau²⁰.

In the following, exemplary cases of malicious cyber activities affecting Rwanda are presented. All cyber incidents gained national and international media attention:

In February 2020, **threat actors targeted a data center that hosted, among others, government servers**. The data center was offline for several hours. A majority of government websites were consequently inaccessible, including the website of president Paul Kagame. The same data center had already been targeted in 2016. Back then, the threat actors compromised the provider, a company that issues video conferencing software used by local Rwandan governments. Sensitive user data was leaked due to the incident.²¹

According to a 2019 report by the Financial Times, vulnerable groups from Rwanda were regularly targeted with the **spyware Pegasus**, which was created by the Israel-based company NSO Group. The program was exploiting vulnerabilities within the Whatsapp call function. The program then infiltrated the target phone and transmitted data like the owner's location or encrypted chats. WhatsApp, who at the time investigated the issue with the University of Toronto's Citizen Lab, quickly closed the exploit. Publicly, NSO has denied any allegations of its software use against members of civil society²².

Key Documents

Rwanda's interests in cyberspace are defined through the following documents²³: the ICT Sector Strategic Plan 2018-2024²⁴, and the National Cyber Security Strategic Plan²⁵, and the the National Cyber Security Policy²⁶.

The **ICT Sector Strategic Plan 2018-2024**²⁷, published by the Ministry of Information Technology and Communications, aims to foster Rwanda's socio-economic development by maximizing the ICT sector's power. Cybersecurity is an integral part of the pursued outcomes and activities to achieve this goal, such as securing Rwanda's cyberspace and information assets²⁸.

Rather than a strategic document, the **National Cyber Security Strategic Plan** of the Republic of Rwanda²⁹, published in 2015, is an implementation framework. It mainly aims to



guide implementation of the National Cyber Security Policy, the National Cyber Security Authority, officially established through Law N. 26/2017, and the National Cyber Security Advisory Board (for more information, see below). The National Cyber Security Strategic Plan defines roles, responsibilities, and priorities for stakeholders involved in the implementation process³⁰.

Following the **National Cyber Security Policy**³¹, implemented by the Ministry of Information Technology & Communications in 2015, Rwanda aims to make its cyberspace secure and resilient. The country's objectives are:

- to build cybersecurity capabilities for detection, prevention, and response to cybersecurity incidents and threats;
- to establish an institutional framework to foster cybersecurity governance and coordination;
- to strengthen legal and regulatory frameworks;
- and to promote research and development, awareness, and national, regional, and international cooperation in cybersecurity.

To achieve the objectives, the National Cyber Security Policy lists policy areas with respective measures that need to be implemented:

- Policy Area 1: Cyber Security Capabilities, e.g., Establish and strengthen National Security and Incident Response Team (Rw-CSIRT);
- Policy Area 2: Institutional Framework for Cyber Security, e.g., Establish Agency in Charge of National Cyber Security and National Cyber Security Advisory Board; Policy Area 3: Cyber Security Legal and Regulatory Framework, e.g., Define Standards and Guidelines;
- Policy Area 4: Critical Information Infrastructure Protection, e.g., Establish a Public-Private Collaboration Framework;
- Policy Area 5: Government Cyber Security Enhancement Program, e.g., Establish Security Levels for Systems, Applications, and Services;
- Policy Area 6: Cyber Security Capacity Building and Awareness, e.g., Develop National Cyber Security Awareness Program;
- Policy Area 7: Building a Cyber Security Industry, e.g., Foster Innovation through Research and Development;
- Policy Area 8: International Cooperation, e.g., Strengthen Regional and International Cooperation.



Legal Frameworks

The primary legislation governing cybersecurity policy in Rwanda are Law N° 60/2018, Law N. 26/2017, and Law N.24/2016³².

The August 2018 Cybercrime Law, **Law N° 60/2018**³³, deals with preventing cybercrime, cybercrime investigation, offenses, and penalties. The law, e.g., highlights the obligation for individuals and entities to collaborate with organs in charge of investigations. The law lays the foundation for the government and the private sector to combat cybercrime affecting Rwanda³⁴. For more information on public critique on the law, please see section “Role of Rwandan Non-Governmental Stakeholders in Cybersecurity: Civil Society”.

Amongst other aspects, **Law N. 24/2016**³⁵ focuses on promoting national Information and Communication Technologies (ICT) policy objectives and establishing objectives for the Information and Communication Technologies industry. The law applies to electronic communications, the information society, the broadcasting, and the postal sector and establishes a framework for ICT policy and regulation.

Law N. 26/2017³⁶ defines the National Cyber Security Authority’s (NCSA) mission and responsibilities, its organization, responsibilities, functioning, property, and finance. Law N. 26/2017 officially established the National Cyber Security Authority.

Cybersecurity Architecture - Selected Institutions

Various institutions work on enhancing cybersecurity in Rwanda, such as the **National Cyber Security Authority (NCSA)**. The NCSA was established to protect Rwanda’s national integrity and security through building cybersecurity skills and capacities³⁷. In September 2020, all cybersecurity activities were officially handed over to NCSA by the Rwanda Information Society Authority, a government institution established in 2017 with a mission is to digitize Rwanda through increased usage of ICT³⁸. The NCSA will be discussed in more depth in the governmental stakeholder spotlight on page 13.

The **Rwanda National Computer Security and Incident Response Team (Rw-CSIRT)** is offered as a service by the National Cyber Security Authority³⁹. It is mandated with preventing and responding to cybersecurity incidents in public and private organizations and raising awareness for the general public. Since its foundation through the Government of Rwanda in 2014, it serves as a national point of contact for computer security incidents coordination and response provides information on cybersecurity threats and vulnerabilities, builds cybersecurity capacities to handle incidents and threats, and promotes information security awareness, research, and development in the field as well as regional and international cooperation⁴⁰. Despite its institutional connection to the NCSA, the Rw-CSIRT has its own operational capacity and takes the lead in national responses to cyber incidents (*information deprived of expert interviews*).



The **National Cyber Security Advisory Board (NCSAB)** advises the NCSA. The NCSAB is an entity consisting of National Cyber Security Organs and private sector representatives. It provides strategic help and guidance on national cybersecurity programs⁴¹.

The **Rwanda Investigation Bureau (RIB)** is an investigative organ with the mandate to perform investigative functions⁴². It is responsible for preventing, detecting, investigating, and responding to criminal threats, among others, cybercrime. To do so, it maintains relationships with other law enforcement agencies. The current RIB Secretary General and the Deputy Secretary General were officially appointed by the President of the Republic of Rwanda⁴³. Among other departments, the RIB has a “Cyber - Crimes Investigation Division”⁴⁴.

The **Rwanda National Police’s Department of Information Technology and Cyber Security** works on information technology and cybersecurity matters⁴⁵. In general, the Rwanda National Policy focuses primarily on countering cyber threats and law enforcement of cyber-crimes, e.g., in cooperation with banks in the country⁴⁶.

The **Rwanda Development Board (RDB)** is a government entity mandated to foster Rwanda’s economic development through private sector growth⁴⁷. In 2009, the government founded an ICT Security Division in the RDB to lead the implementation of the national cybersecurity programs⁴⁸. Today, the ICT Security Division is responsible for ensuring “efficient cyber-crime preparedness, response, reporting, risk management and policy compliance across government institutions”⁴⁹. It is also responsible for maintaining the security of “Rwanda’s critical IT infrastructure, systems, and information assets”⁵⁰, leading the implementation of ICT security strategic plans for the government and developing information security legal frameworks. The Rwanda Development Board has also joined CAMP⁵¹, the Cybersecurity Alliance for Mutual Progress, together with the Rwanda National Policy⁵².

The **Rwanda Information Society Authority (RISA)**, a government institution derived from the IT department of Rwanda Development Board with a mission is to digitize Rwanda through increased usage of ICT, used to be responsible for cybersecurity matters. It officially handed over all cybersecurity matters to NCSA in 2020⁵³. RISA still informs citizens on important National Cyber Security Alerts⁵⁴.

Governmental Stakeholder Spotlight: The National Cyber Security Authority

This spotlight explores the responsibilities, responsibilities, and communication of a central government authority that supervises cybersecurity and incident response. In Rwanda, the National Cyber Security Authority (NCSA) has the mandate to protect Rwanda’s national integrity and security through building cybersecurity skills and capabilities. Its responsibilities are, among others, to advise the president and other public and private institutions on strategies to defend the country’s interests in cyberspace; to conduct cyber intelligence on any national security threat in cyberspace, and to prevent cyber incidents in order to protect ICT infrastructure in general and critical information infrastructure in particular. To fulfill these tasks, the NCSA enjoys full financial and administrative autonomy⁵⁵.



As a government agency, it maintains strong relationships with other government entities. The Directives on Cyber Security for Network and Information Systems to all Public Institutions by the Rwanda Information Society Authority, published in June 2018, underpins the relationship between NCSA and other government entities. The Directive is meant to provide instructions and guidelines for securing the government's ICT infrastructure. Therefore, all entities must implement minimum security controls before connecting to the internet, making the NCSAs consultation increasingly important⁵⁶.

The NCSA also supports other government entities with the implementation of the National Cyber Security Policy and maintains contact with the President, whom it advises on cybersecurity matters, as well as the Prime Minister (and his Cabinet), who appoints certain NCSA's roles⁵⁷. As per Law No 26/2017, the NCSA also advises and cooperates with other Rwandan public and private institutions, particularly on strategies to defend Rwanda's interests in cyberspace as well as the implementation and monitoring of ICT security, ICT policy, and programs. Law No 26/2017 also provides the NCSA with the responsibility of conducting cyber intelligence and providing relevant information to the relevant Rwandan organs⁵⁸.

The NCSA public communication is an integral part of its stakeholder management. It mainly communicates through its website. It offers a range of services, such as alerts on cybersecurity threats or information on upcoming events and awareness campaigns about cybersecurity in Rwanda and the region⁵⁹.

The Private Sector

Non-governmental stakeholders working in and operating in cybersecurity consist of stakeholders from the private sector and civil society in Rwanda.

The Rwandan market is a growing economy. Rwanda's private sector, therefore, consists of various enterprises in different sectors, such as the energy or financial sector⁶⁰. The Rwandan financial sector is build of a "vast and growing array of institutions, a stock exchange, banks, (...) insurance companies"⁶¹, and other organizations.

Among these institutions is the state-owned National Bank of Rwanda (BNR), established in 1964, which has the main objectives of ensuring price stability and establishing binding regulations for Rwandan financial institutions⁶². The National Bank of Rwanda is the supervisor and regulator of the banking system in Rwanda. To fulfill this purpose, the BNR maintains relationships with other national banks that are meant to adhere to norms and protection of depositors through legal and regulatory frameworks of the National Bank of Rwanda⁶³. As a state-owned bank with the power to set financial regulations, the Bank also works closely with the Rwandan government⁶⁴. Its work is part of the government's broader strategy of being a financial sector hub⁶⁵.

The main cyber regulation affecting the BNR is the 2018 Regulation on Cybersecurity, which aims to (1) establish minimum standards to banks for their protection against cy-



bersecurity threats, and (2) promote the protection of customer information and information technology systems of banks⁶⁶. In brief, the regulation lays out requirements for governance, reporting, procedures, and training that all financial institutions must put in place. The main requirements are, among others, to have a cybersecurity governance framework including a cyber strategy, governance program, policy standards, clear organizational structure, metrics & monitoring, and an incident response plan; to notify the central bank within two hours of the discovery of an incident, with an incident report submitted within 24 hours, and to have periodic penetration testing and vulnerability assessments⁶⁷. In addition, independent of the BNR's regulations, some banks in Rwanda have their own Computer Emergency Response Teams to counter cyber incidents (*information deprived of expert interviews*).

Civil Society

Civil society organizations play a role for cybersecurity (policy) in Rwanda. One civil society organization active in cybersecurity is the Africa Cybersecurity Consortium (ACC), originally named the Rwanda Cybersecurity Consortium. Its main objectives are helping organizations collaborate on cybersecurity and developing cutting-edge cybersecurity skills and knowledge. Its primary responsibilities are, for example, (1) to ensure the access of Africans to opportunities such as partnership, training, research, consultancy, advocacy, certification, mentorship, or job opportunities in cybersecurity; (2) to ensure that non-governmental organizations and the general public are aware of cybercrime news, information security issues, and the associated risks; or (3) to support in identifying and addressing emerging cybersecurity challenges in Rwanda⁶⁸.

More broadly, according to European External Action Service analysis⁶⁹, Rwandan civil society organizations often act as implementing partners for government processes or outputs rather than constituting an active influence on public policies. A more active role and participation in governmental decision-making and implementation processes would be necessary, particularly for enhancing trust between and among public authorities and citizens of Rwanda⁷⁰.

Civil society organizations, however, are engaged with cybersecurity policy-making and voiced their opinion on legislative proposals in the past. According to critics⁷¹, the August 2018 Cybercrime Law (see “Legal Framework” section)⁷², for example, limits space for online expression⁷³. Freedom House, among other sources, states that the law could be used to target, fine, or imprison vulnerable groups in the country. Vulnerable groups can, for example, be targeted for spreading “rumors” on the basis of the law's provisions. This has led to arrests of journalists in the past⁷⁴.

Civil society is further affected by surveillance. Even though the extent of surveillance is unknown, critics argue that it is enabled by measures such as new SIM card registration requirements that prohibit the use of more than three SIM cards per person and network. Journalists, government critics, and other users are further intimidated on social media on a regular basis⁷⁵.



Bilateral and Multilateral Cooperation

Rwanda is a member of the African Union, the Commonwealth, the International Telecommunications Union, and the United Nations⁷⁶. All these international organizations deal with and discuss cybersecurity-related topics. The African Union, for example, adopted the African Union Convention on Cyber Security and Personal Data Protection in 2014 to address cybersecurity and cybercrime⁷⁷, which was ratified by Rwanda in 2019⁷⁸, while the International Telecommunications Union works with member states on enhancing cyber capacity. It, e.g., helps countries to strengthen their National Computer Incident Response Teams⁷⁹.

Rwanda National Police and the Rwanda Development Board represent Rwanda in the **Cybersecurity Alliance for Mutual Progress (CAMP)**⁸⁰, which serves as a network platform to enhance the level of cybersecurity of its members through sharing development experiences and trends of cybersecurity⁸¹.

Rwanda also **joined cooperation with Israel and several other African countries (Zambia, Ethiopia, Uganda, South Sudan, Rwanda, Kenya, Tanzania)** agreeing to cooperate on matters of security, including cybersecurity⁸².

Rwanda signed a **Memorandum of Understanding on Cyber Security Framework for Cooperation and Collaboration between the Northern Corridor Integration Projects Partner States**, the Republic of Kenya, Rwanda, South Sudan, and Uganda in 2015⁸³. The Memorandum of Understanding acknowledges the global rise of cyber threats and aims to enhance cooperation between the member states. It includes the establishment of a Northern Corridor CIRT, a collaborative framework to share cybersecurity information and coordinate incident handling, building technical capabilities, and enhancing research and development capacities⁸⁴.

It is also a member of the **Global Forum on Cyber Expertise**. The Global Forum on Cyber Expertise consists of countries, intergovernmental and international organizations, and private companies that aim to contribute to cyber capacity.⁸⁵



Sources

- 1 Auswärtiges Amt (2020): Ruanda: Steckbrief. <https://www.auswaertiges-amt.de/de/aussenpolitik/laender/ruanda-node/ruanda/212024>
- 2 Auswärtiges Amt (2021): Ruanda: Politisches Porträt. <https://www.auswaertiges-amt.de/de/aussenpolitik/laender/ruanda-node/politisches-portraet/212068>
- 3 The World Bank (2020): Population, total – Rwanda. <https://data.worldbank.org/indicator/SP.POP.TOTL?locations=RW>
- 4 Bishumba, The New Times (2017): MPs approve law making Swahili official language. <https://www.newtimes.co.rw/section/read/207840>
- 5 National Bank of Rwanda: Exchange Rate. <https://www.bnr.rw/currency/exchange-rate/>
- 6 Auswärtiges Amt (2020): Ruanda: Steckbrief. <https://www.auswaertiges-amt.de/de/aussenpolitik/laender/ruanda-node/ruanda/212024>
- 7 Auswärtiges Amt (2020): Ruanda: Steckbrief. <https://www.auswaertiges-amt.de/de/aussenpolitik/laender/ruanda-node/ruanda/212024>
- 8 The World Bank (2021): The World Bank in Rwanda. <https://www.worldbank.org/en/country/rwanda/overview#1>
- 9 Government of the Republic of Rwanda (2021): About the Parliament. <https://www.parliament.gov.rw/about-1>
- 10 Auswärtiges Amt (2021): Ruanda: Politisches Porträt. <https://www.auswaertiges-amt.de/de/aussenpolitik/laender/ruanda-node/politisches-portraet/212068>
- 11 The World Bank (2021): The World Bank in Rwanda. <https://www.worldbank.org/en/country/rwanda/overview#1>
- 12 Government of Rwanda (2017): Rwanda 7 Years Government Programme: National Strategy for Transformation (NST 1), 2017 – 2024. <https://www.greengrowthknowledge.org/national-documents/rwanda-7-years-government-programme-national-strategy-transformation-nst-1-2017-%E2%80%93>
- 13 World Bank Group (2020): Accelerating Digital Transformation in Rwanda, Rwanda Economic Update. <https://webcache.googleusercontent.com/search?q=cache:yqcpz-tCVQf8J:https://documents.worldbank.org/curated/en/912581580156139783/pdf/Rwanda-Economic-Update-Accelerating-Digital-Transformation-in-Rwanda.pdf+&c-d=2&hl=de&ct=clnk&gl=de&client=firefox-b-e>
- 14 World Bank Group (2020): Accelerating Digital Transformation in Rwanda, Rwanda Economic Update. [This document is exercise-specific information material and was developed for the purpose of a cybersecurity policy exercise only.](https://webcache.googleusercontent.com/search?q=cache:yqcpz-</div><div data-bbox=)



[tCVQf8J:https://documents.worldbank.org/curated/en/912581580156139783/pdf/Rwanda-Economic-Update-Accelerating-Digital-Transformation-in-Rwanda.pdf+%&cd=2&hl=de&ct=clnk&gl=de&client=firefox-b-e](https://documents.worldbank.org/curated/en/912581580156139783/pdf/Rwanda-Economic-Update-Accelerating-Digital-Transformation-in-Rwanda.pdf+%&cd=2&hl=de&ct=clnk&gl=de&client=firefox-b-e)

- 15 *Xinhuanet (2019): Rwanda's Internet penetration rate reaches 52.1 pct in 2018. <http://www.xinhuanet.com/>*
- 16 The World Bank (2021): The World Bank in Rwanda. <https://www.worldbank.org/en/country/rwanda/overview#1>
- 17 Auswärtiges Amt (2021): Ruanda: Politisches Porträt. <https://www.auswaertiges-amt.de/de/aussenpolitik/laender/ruanda-node/politisches-portraet/212068>
- 18 Reporters Without Borders (2021): Rwanda. <https://rsf.org/en/rwanda>
- 19 Mwai, The New Times (2020): Cybersecurity: Majority of Rwandan SMEs vulnerable. <https://www.newtimes.co.rw/news/cybersecurity-majority-rwandan-smes-vulnerable>
- 20 Côme Mugisha, The New Times (2020): Cybercrimes increased by 70 % during lockdown – RIB. <https://www.newtimes.co.rw/news/cybercrimes-increased-70-during-lockdown-rib>
- 21 Taarifa (2020): Government Data Center Goes Down, President's Website Off. <https://taarifa.rw/government-data-center-goes-down-presidents-website-off/>
- 22 Srivastava/Wilson, Financial Times (2019): Inside the WhatsApp hack: how an Israeli technology was used to spy. <https://www.ft.com/content/d9127eae-f99d-11e9-98fd-4d6c20050229>
- 23 UNIDIR (2020): Rwanda. <https://webcache.googleusercontent.com/search?q=cache:RpFzf5RF-yYJ:https://unidir.org/cpp/en/state-pdf-export/eyJjb3VudHJ5X2dyb-3VwX2lkjoiMzgifQ+%&cd=2&hl=de&ct=clnk&gl=de&client=firefox-b-e>
- 24 Republic of Rwanda Ministry of Information Technology and Communications (2017): ICT Sector Strategic Plan (2018-2024). https://www.minecofin.gov.rw/fileadmin/user_upload/Minecofin/Announcements/ICT.pdf
- 25 Republic of Rwanda (2015): National Cyber Security Strategic Plan. https://risa.rw/file-admin/user_upload/Others%20documents/National_Cyber_Security_Strategic_Plan_Rwanda.pdf
- 26 RISA (2015): National Cyber Security Policy. https://www.risa.rw/fileadmin/user_upload/Others%20documents/National_Cyber_Security_Policy_Rwanda.pdf
- 27 Republic of Rwanda Ministry of Information Technology and Communications (2017): ICT Sector Strategic Plan (2018-2024). https://www.minecofin.gov.rw/fileadmin/user_upload/Minecofin/Announcements/ICT.pdf



- 28 UNIDIR (2020): Rwanda. <https://webcache.googleusercontent.com/search?q=-cache:RpFzf5RF-yYJ:https://unidir.org/cpp/en/state-pdf-export/eyJjb3VudHJ5X2dyb-3VwX2lkljoiMzgifQ+&cd=2&hl=de&ct=clnk&gl=de&client=firefox-b-e>
- 29 Republic of Rwanda (2015): National Cyber Security Strategic Plan. https://risa.rw/fileadmin/user_upload/Others%20documents/National_Cyber_Security_Strategic_Plan_Rwanda.pdf
- 30 UNIDIR (2020): Rwanda. <https://webcache.googleusercontent.com/search?q=-cache:RpFzf5RF-yYJ:https://unidir.org/cpp/en/state-pdf-export/eyJjb3VudHJ5X2dyb-3VwX2lkljoiMzgifQ+&cd=2&hl=de&ct=clnk&gl=de&client=firefox-b-e>
- 31 RISA (2015): National Cyber Security Policy. https://www.risa.rw/fileadmin/user_upload/Others%20documents/National_Cyber_Security_Policy_Rwanda.pdf
- 32 UNIDIR (2020): Rwanda. <https://webcache.googleusercontent.com/search?q=-cache:RpFzf5RF-yYJ:https://unidir.org/cpp/en/state-pdf-export/eyJjb3VudHJ5X2dyb-3VwX2lkljoiMzgifQ+&cd=2&hl=de&ct=clnk&gl=de&client=firefox-b-e>
- 33 Rura (2018): Law N° 60/2018 OF 22/8/2018 on Prevention and Punishment of Cyber crimes. https://rura.rw/index.php?id=104&tx_news_pi1%5Bnews%5D=603&tx_news_pi1%5Bday%5D=27&tx_news_pi1%5Bmonth%5D=9&tx_news_pi1%5B-year%5D=2018&cHash=cf6a0de5282574dd3c3a8081a6348b83
- 34 UNIDIR (2020): Rwanda. <https://webcache.googleusercontent.com/search?q=-cache:RpFzf5RF-yYJ:https://unidir.org/cpp/en/state-pdf-export/eyJjb3VudHJ5X2dyb-3VwX2lkljoiMzgifQ+&cd=2&hl=de&ct=clnk&gl=de&client=firefox-b-e>
- 35 Rura: Laws and Regulations. <https://rura.rw/index.php?id=50>
- 36 Republic of Rwanda (2017): Law N. 26/2017. https://cyber.gov.rw/fileadmin/user_upload/NCSA/Documents/Laws/Law_establishing_the__NCSA__1_.pdf
- 37 Republic of Rwanda (2017): Law N. 26/2017. https://cyber.gov.rw/fileadmin/user_upload/NCSA/Documents/Laws/Law_establishing_the__NCSA__1_.pdf
- 38 Twitter (2020): Ministry of ICT and Innovation | Rwanda. <https://twitter.com/rwandaict/status/1305884557015736320>
- 39 National Cyber Security Authority: Rw-CSIRT. <https://cyber.gov.rw/rw-csirt/>
- 40 * Rw-CSIRT: About Us. <https://cyber.gov.rw/about-ncsa> *
- 41 Republic of Rwanda (2015): National Cyber Security Strategic Plan. https://risa.rw/fileadmin/user_upload/Others%20documents/National_Cyber_Security_Strategic_Plan_Rwanda.pdf
- 42 Rwanda Investigation Bureau: History. <https://www.rib.gov.rw/index.php?id=24;%20https://www.rib.gov.rw/index.php?id=293>



- 43 Rwanda Investigation Bureau: History. <https://www.rib.gov.rw/index.php?id=24;%20https://www.rib.gov.rw/index.php?id=293>
- 44 Rwanda Investigation Bureau: RIB Leadership Structure. <https://www.rib.gov.rw/index.php?id=23>
- 45 Rwanda National Police: RNP Organizational Structure. <https://police.gov.rw/about-rnp/organisational-structure/>
- 46 Rwanda National Police: [PHOTOS]: Banks, Telecoms, Police in a new synergy to counter cyber threats. https://police.gov.rw/media-archives/news-detail/?tx_news_pi1%5B-news%5D=8995&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&cHash=0f43112a4d5c9d78737959b22fa17915
- 47 Rwanda Development Board: About RDB. <https://rdb.rw/about-rdb/#overview>
- 48 Rwanda Development Board: Information communication technology. <https://rdb.rw/departments/information-communication-technology/>
- 49 Rwanda Development Board: Information communication technology. <https://rdb.rw/departments/information-communication-technology/>
- 50 Rwanda Development Board: Information communication technology. <https://rdb.rw/departments/information-communication-technology/>
- 51 CAMP: Members. <https://www.cybersec-alliance.org/camp/membership.do>
- 52 CAMP: About CAMP. <https://www.cybersec-alliance.org/camp/about.do>
- 53 Twitter (2020): Ministry of ICT and Innovation | Rwanda. <https://twitter.com/rwandaict/status/1305884557015736320>
- 54 RISA: Alert. https://www.risa.rw/fileadmin/user_upload/Archive/Alert__Critical_Vulnerability_in_Oracle_WebLogic_.pdf
- 55 Republic of Rwanda (2017): Law N. 26/2017. https://cyber.gov.rw/fileadmin/user_upload/NCSA/Documents/Laws/Law_establishing_the__NCSA__1_.pdf
- 56 RISA (2015): National Cyber Security Policy. https://www.risa.rw/fileadmin/user_upload/Others%20documents/National_Cyber_Security_Policy_Rwanda.pdf
- 57 Republic of Rwanda (2017): Law N. 26/2017. https://cyber.gov.rw/fileadmin/user_upload/NCSA/Documents/Laws/Law_establishing_the__NCSA__1_.pdf; Twitter (2020): Office of the PM | Rwanda. <https://twitter.com/PrimatureRwanda/status/1332435088861171714>
- 58 Republic of Rwanda (2017): Law N. 26/2017. https://cyber.gov.rw/fileadmin/user_upload/NCSA/Documents/Laws/Law_establishing_the__NCSA__1_.pdf
- 59 NCSA: Home. <https://cyber.gov.rw/home/>



- 60 International Trade Administration (2021): Rwanda - Country Commercial Guide. <https://www.trade.gov/country-commercial-guides/rwanda-market-overview>
- 61 Rwanda Development Board (n.d.): Financial services. <https://rdb.rw/investment-opportunities/financial-services/>
- 62 National Bank of Rwanda: Vision and Mission. <https://www.bnr.rw/about/vision-and-mission/>
- 63 National Bank of Rwanda: Banking. <https://www.bnr.rw/index.php?id=228>
- 64 National Bank of Rwanda: Bank Supervision. <https://www.bnr.rw/financial-stability/bank-supervision/>
- 65 Foreign, Commonwealth & Development Office: The political economy of central bank effectiveness: The case of National Bank of Rwanda. <https://www.gov.uk/research-for-development-outputs/the-political-economy-of-central-bank-effectiveness-the-case-of-national-bank-of-rwanda>
- 66 National Bank of Rwanda: Regulations. https://www.bnr.rw/laws-and-regulations/banking/regulations/?tx_bnrdocumentmanager_frontend%5Baction%5D=activeList&tx_bnrdocumentmanager_frontend%5Bcontroller%5D=Document&tx_bnrdocumentmanager_frontend%5B%40widget_0%5D%5BcurrentPage%5D=2&cHash=e47
- 67 National Bank of Rwanda: Regulations. https://www.bnr.rw/laws-and-regulations/banking/regulations/?tx_bnrdocumentmanager_frontend%5Baction%5D=activeList&tx_bnrdocumentmanager_frontend%5Bcontroller%5D=Document&tx_bnrdocumentmanager_frontend%5B%40widget_0%5D%5BcurrentPage%5D=2&cHash=e47
- 68 Africa Cybersecurity Consortium: Vision & Mission. https://africacybersecure.org/?page_id=33
- 69 Constantini, Verdecchia, Rutayisire (2013): MAPPING OF THE CIVIL SOCIETY AND PROJECT IDENTIFICATION OF A SUPPORT PROGRAM TO THE CIVIL SOCIETY IN RWANDA. https://eeas.europa.eu/archives/delegations/rwanda/documents/press_corner/mapping-of-the-civil-society-and-project-identification_en.pdf
- 70 Constantini, Verdecchia, Rutayisire (2013): MAPPING OF THE CIVIL SOCIETY AND PROJECT IDENTIFICATION OF A SUPPORT PROGRAM TO THE CIVIL SOCIETY IN RWANDA. https://eeas.europa.eu/archives/delegations/rwanda/documents/press_corner/mapping-of-the-civil-society-and-project-identification_en.pdf
- 71 Freedom House (2019): Rwanda. <https://freedomhouse.org/country/rwanda/freedom-net/2019>
- 72 Rura (2018): Law N° 60/2018 OF 22/8/2018 on Prevention and Punishment of Cyber crimes. https://rura.rw/index.php?id=104&tx_news_pi1%5Bnews%5D=603&tx_news_pi1%5Bday%5D=27&tx_news_pi1%5Bmonth%5D=9&tx_news_pi1%5B-year%5D=2018&cHash=cf6a0de5282574dd3c3a8081a6348b83



- 73 Freedom House (2019): Rwanda. <https://freedomhouse.org/country/rwanda/freedom-net/2019>
- 74 Freedom House (2019): Rwanda. <https://freedomhouse.org/country/rwanda/freedom-net/2019>
- 75 Freedom House (2019): Rwanda. <https://freedomhouse.org/country/rwanda/freedom-net/2019>
- 76 UNIDIR (2020): Rwanda. <https://webcache.googleusercontent.com/search?q=-cache:RpFzf5RF-yYJ:https://unidir.org/cpp/en/state-pdf-export/eyJjb3VudHJ5X2dyb-3VwX2lkIjoiMzgifQ+&cd=2&hl=de&ct=clnk&gl=de&client=firefox-b-e>
- 77 CCDCOE: African Union. <https://ccdcoe.org/organisations/au/>
- 78 Nkusi, The New Times (2019): AU Convention is finally part of Rwandan law. <https://www.newtimes.co.rw/opinions/au-convention-finally-part-rwandan-law>
- 79 ITU: National CIRT. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx>
- 80 CAMP: About CAMP. <https://www.cybersec-alliance.org/camp/about.do>
- 81 CAMP: About CAMP. <https://www.cybersec-alliance.org/camp/about.do>
- 82 Lukastime: Israel and 7 African countries agree to collaborate on security and economic matters. <https://www.lusakatimes.com/2016/07/05/israel-and-7-african-countries-agree-to-collaborate-on-security-and-economic-matters/>
- 83 UNIDIR (2020): Rwanda. <https://webcache.googleusercontent.com/search?q=-cache:RpFzf5RF-yYJ:https://unidir.org/cpp/en/state-pdf-export/eyJjb3VudHJ5X2dyb-3VwX2lkIjoiMzgifQ+&cd=2&hl=de&ct=clnk&gl=de&client=firefox-b-e>
- 84 allAfrica (2015): Kenya: Memorandum of Understanding On Cyber Security Framework for Co-Operation and Collaboration Between the Northern Corridor Integration Projects Partner States to Prevent and Respond to Evolving Cyber Security Threats. <https://allafrica.com/stories/201504270455.html>
- 85 GFCE: Member Profile Page Rwanda. <https://thegfce.org/member/rwanda/>