# Internet Infrastructure Security Guidelines for the Arab States

Internet Society

March 2020

## Executive Summary

As many Arab states continue to modernize and diversify their economies with a focus on digital services, trade and e-government, both the opportunities and threats of the Internet are amplified.[1] With more dependence now on the internet in economy, society and critical information infrastructure, maintaining Internet connectivity is essential. To do this, countries need to focus not just on cybersecurity, but specifically on policies, technologies and best practices that strengthen the security of Internet infrastructure.

How we approach cybersecurity is changing. The most up to date regional cybersecurity frameworks do not concentrate on *security as the end-goal*, but rather on *making security facilitate overall social and economic goals*. Cybersecurity today does not aim to close off infrastructure - "building moats and pulling up the drawbridge". It focuses on the role of security in facilitating an interconnected and interdependent global digital economy. The best way to do this is to work collaboratively.

The Internet is made up of independent networks that interconnect using open standards to ensure interoperability. Internet infrastructure includes protocols and services, software and hardware, network interconnection, communication infrastructure, information and is supported with human resources. As the Internet is a 'network of networks', focusing purely on *national* network resilience will not ensure ongoing connectivity; *regional* Internet resilience needs to be the goal.

### Key principles:

Guided by regional experts, and international and regional frameworks on cybersecurity, the Internet Society has identified these essential principles to secure the Internet:

- **Awareness** - Stakeholders in both the public and private sectors need to understand the security risks, as well as how they and others in the Internet infrastructure ecosystem are impacted by these risks.

[1] https://gulfif.org/the-new-battlefront-cyber-security-across-the-gcc/

- **Responsibility** - Each stakeholder should take responsibility for the management of security risks within their respective roles and organizations, taking into account the potential impact of their action or inaction on others.

- **Collaboration** - All stakeholders, including those across borders, must be included in an ongoing cybersecurity dialogue to effectively counter new and persistent threats.

- **Fundamental Rights and Internet Properties** - All stakeholders' actions to manage security risks should adhere to fundamental rights, be transparent, and not infringe upon the Internet properties of voluntary collaboration, open standards, reusable technology building blocks, integrity, permission-free innovation and global reach.[2]

Policies and strategies should include consideration of their impact on the underlying architecture of the Internet and ensure that they do not negatively impact the openness, innovation, and global reach of the Internet.

## The security landscape in the Arab states:

Some key aspects of the current security landscape in the Arab states are:

- National cybersecurity strategies have not been implemented in all countries. They tend to be under-resourced and often focused on a more "top-down control" models than the more up to date collaborative approach.

- Computer Security Incident Response Teams (CSIRTS) (also known as Computer Emergency Response Teams, or CERTs) tend to have less collaboration with the private sector and other stakeholders than in other regions. More collaborative relationships are needed to improve information-sharing, vulnerability-disclosure, capacity-building and incident response.

- Internet infrastructure security and resilience lag in some other regions, but there is an appetite for more cooperative and multi-sectoral partnerships that will allow the public and private sectors to work together.

## Recommendations:

Governments and other stakeholders should empower organizations and institutions to create a collaborative culture of Internet infrastructure security for economic and social prosperity.

**Nationally,** Governments should foster an open, collaborative and resilient Internet security ecosystem that includes:

- Identifying and protecting critical information infrastructure
- Improving Internet infrastructure resilience by facilitating deployment of security standards and best practices
- Improving Internet infrastructure resilience through better network interconnection
- Facilitating information exchange and relationship-building across all stakeholders

[2] https://www.internetsociety.org/internet-invariants-what-really-matters

- Establishing and strengthening national-level Computer Security Incident Response Teams (CSIRTs),
- Using public institutions to lead by example
- Identifying and addressing legal barriers to information-sharing (including supporting ‘white hat’ security researchers) and research on security vulnerabilities, incidents and threats.

**Regionally,** Governments should work with all stakeholders to strengthen regional collaboration:

- Establish a regional group of security experts from government, business, technical, academic and civil society to provide non-binding guidance to the region on Internet infrastructure security issues as needed.
- Participate in and deepen existing communication and coordination cybersecurity initiatives, including consideration of whether to establish a regional threat intelligence-sharing platform
- Pool CSIRT resources where possible, for example, coordinating and sharing training courses between CSIRTs – to increase knowledge and experience and to build cross-border relationships between professionals that build trust for further collaboration
- Increase resiliency of the networks to attacks and outages by facilitating diversity of interconnections between networks, nationally, regionally and internationally.

# Table of Contents

# Introduction

Cybersecurity threats and incidents are increasing, and as the Arab economies become integrated into the global Internet, they share its risks as well as its benefits. Governments have a challenging but essential role to play. They need to reduce and mitigate the risks posed by threats on the Internet, while also maintaining people's trust in it. If people lose trust in the Internet, their economies will lose its dynamic capacity for innovation and growth. The best way to maintain trust in the Internet and harness all the necessary resources to protect it is to work collaboratively across the economy. To do this, governments, Internet infrastructure providers and other security experts need to work together to identify and protect the Internet's infrastructure in the region, while preserving the Internet's fundamental properties as an open trustworthy, secured platform for all.

**Collaborative Security Approach**
The collaborative security approach to Internet security recognizes that people are what ultimately hold the Internet together. The Internet's development has been based on voluntary cooperation and collaboration. Cooperation and collaboration remain the essential factors for its prosperity and potential. The approach emphasizes five principles:

- Preserving opportunities and building confidence;
- Collective responsibility;
- Security solutions fully integrated with rights and the open Internet;
- Security solutions grounded in experience, developed by consensus and evolutionary in outlook; and
- Targeting the point of maximum impact – think globally, act locally.

https://www.internetsociety.org/collaborativesecurity/

This document builds on the results of consultation with regional experts to offer guidance on how to secure Internet infrastructure collaboratively, with appropriate transparency, and safeguarding basic rights and the fundamental properties of the Internet. These guidelines draw on best practices from regional frameworks around the world, including the OECD's Digital Security Risk Management for Economic and Social Prosperity, the European Union's National Cyber Security Strategy Good Practice Guide, and Internet Infrastructure Security Guidelines for Africa; A joint initiative of the Internet Society and the Commission of the African Union.

Regional frameworks have been chosen because they are flexible and practical. They provide relevant best practice and global principles. These guidelines are aimed at policymakers, regulators, and directors of CSIRTs and their affiliated organizations in the Arab states, as well as private sector infrastructure operators such as Internet Service Providers (ISPs). These guidelines respond to the unique cybersecurity challenges and opportunities highlighted by regional experts and consultations in the Arab states.

## Why use the collaborative security approach?

Governments have a key role to play in leading by example and encouraging information-sharing and collaboration at both national and regional levels. But as the Internet is a network of networks without centralized control, and is owned or operated by many different entities, its security cannot be maintained by any single entity. Cooperation and collaboration built the Internet and are the most effective way to protect it.

## A new approach to Internet infrastructure security

Over the last decade, there has been an evolution in the basic approach to cybersecurity. Security is no longer seen as an end-goal in itself, but as something to facilitate social and economic activities. There is now wide recognition that the "moats and drawbridges" approach – simply building higher walls around systems and services - just does not work in a global, interconnected and interdependent economy. This new approach is mirrored in the more successful national frameworks and strategies where openness and collaboration are the foundation.

### What these guidelines do and do not focus on

These guidelines focus on how to identify, protect and sustain Internet infrastructure in today's threat environment. Today, key services such as utilities and health systems depend on a secure and functioning Internet. These guidelines focus on Internet infrastructure security, not overall cybersecurity.

The guidelines do not deal directly with national security, nation-sanctioned cyber-attacks, cyberwarfare, and cybercrime. These issues are largely dealt with by different international instruments including, for example, the Budapest Convention on Cybercrime. Nonetheless, implementing these guidelines on Internet infrastructure security will increase an economy's overall resilience to a wide range of threats and attacks.

These guidelines are not the final answer to every issue, but their collaborative approach is an essential first step towards resilient, safe and secure Internet infrastructure.

## 1 The Security Threat and Capability Landscape in the Arab States

The nature and types of threats prevalent in the Arab states are fundamentally similar to those faced around the world. Increasing cyber threats and attacks are driven by state actors, financially-oriented criminal activity, hacktivism, and terrorism. While this region generally lags behind Europe and the Asia-Pacific on capabilities and coordination,3 it is moving quickly to catch up. Broad regional observations are:

- **Significant geopolitical threats**
  The threat landscape is distinct from other regions with a high degree of threat from external state actors[4] and relatively low levels of preparedness.[5] Countries such as Sudan, Egypt, Iraq, and Libya appear to be targeted because of the overall weakness of their network security.
- **Data breaches – low reporting and high costs**
  There is relatively low reporting of security and data breaches[6], masking both the likely number and scope of actual breaches. The cost of breaches is rising, with Saudi Arabia and the United Arab Emirates joining the US as the three countries with the most costly data breaches in the world, averaging over $5 million USD to remedy each breach.[7] Added to this, the comparatively long periods of time required to remedy breaches suggests information-sharing and vulnerability disclosure incentives are not as well aligned between national stakeholders as they could be. Compared to other regions, where data breaches tend to concern personal and financial data, breaches in the Middle East often concerned trade and state secrets.[8]
- **CSIRTs emerging and primarily state-led**
  Most countries have established centres to build cyber security capacity and respond to immediate incidents and threats. However, they tend to have less collaboration with the private sector and other stakeholders than in other regions, creating challenges for relationship-building

[5] https://www.pwc.com/m1/en/publications/documents/middle-east-cyber-security-survey.pdf

[4] https://gulfnews.com/world/gulf/saudi/gulf-states-at-risk-of-cyber-attacks-1.1985345

[5] http://www.eiu.com/industry/article/806588464/cyber-attacks-is-the-gcc-prepared/2018-04-03

[6] http://www.securitymea.com/2019/07/01/darkmatter-group-releases-mena-cybersecurity-report/

[7] https://www.ibm.com/security/data-breach

[8] https://infowatch.com/sites/default/files/report/analytics/a_study_of_data_leaks_in_the_middle_east_in_2017-2018_.pdf

and vulnerability disclosure. Sectoral CSIRTs are beginning to be established in some countries, e.g. in the telecoms or energy sectors.

- **Skills are still in development, particularly advanced skills**
  Cybersecurity capacity at an advanced level, i.e. specialized university and post-graduate education, is still at a relatively low level. Most countries in the region offer professional cybersecurity training, but at levels significantly below the availability in other regions such as Europe or the Asia-Pacific.[9]

Our consultations in several Arab countries show there is a high level of awareness of these issues and strong motivation to address them by further developing the necessary national and regional relationships, governance. and operational capacity.

# 2 Core Elements of Internet Infrastructure

The Internet is made up of independent networks that connect to one another using open Internet standards that ensure interoperability. Internet infrastructure is the element that makes up and enables the movement of usable data across those networks. As so much of a country's economy, society and essential services now depend on the Internet, the top priority is to maintain connectivity.

The six **Core Elements of Internet Infrastructure** are:

## Protocols and Services

Protocols are technical standards that allow different computer systems to communicate. A key example of a protocol is the TCP/IP[10] suite that is the foundation of the Internet.

Services in this context are the functionalities that make the Internet so engaging and useful by facilitating the exchange of Internet traffic. Internet infrastructure services include addressing – the global domain name resolution system that uses Domain Name System (DNS) – which allows us to navigate the Internet. They also include functions like routing, using the Border Gateway Protocol (BGP), and application services like the World Wide Web. Internet infrastructure services are distinct from the user services that sit 'on top of' them, such as browsers, search engines and social media.

Protocols and services are fundamental to Internet infrastructure security, because without them we cannot send and receive data, navigate the Internet to access and share information, or communicate with each other.

Arab context: Security threats to protocols and services include domain-hijacking. One recent threat was the "Sea Turtle" campaign, 2017 to 2019, that appeared to target public and private sector organizations in the Middle East and North Africa. The attackers accessed the DNS records of well-known organizations and changed them to point users to servers under the hackers' control. The websites' users were then misdirected to included false "military organizations, national security agencies, foreign affairs ministries and energy companies in Libya, Egypt, United Arab Emirates, Cyprus, Lebanon, Iraq, Jordan, Turkey, Armenia, Syria and Albania." [11]

[9] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[10] TCP (Transfer Control Protocol) and IP (Internet Protocol) are maintained by the Internet Engineering Task Force, an open standards body. https://en.wikipedia.org/wiki/Internet_protocol_suite

[11] https://www.infosecurity-magazine.com/news/dns-hijackers-target-middle-east-1-1/

## Software and Hardware

Software in this context includes operating systems and firmware. Software products have security vulnerabilities that need to be addressed through regular updating, patching and other methods.

Hardware is machines or wiring, including network devices (switches, routers, firewalls, and gateways); servers, and end-user devices (personal computers, tablets, mobile phones).

Arab context: Ransomware attacks, typically based on software update issues, are common – the Kingdom of Saudi Arabia and United Arab Emirates are the most attacked of the Arab countries[12]. For hardware, user device vulnerabilities are an issue, for example, with phishing attacks on officials' infected phones to collect call records, audio recordings, device location information and text messages.[13]

## Network Interconnection

The Internet is a "network of networks", so the technologies and services that provide the interconnection between these networks are critical. These are sometimes provided by Internet Exchange Points (IXPs) – a facility where different IP networks meet to exchange local traffic with each other via a switch. Both Internet Service Providers (ISPs) and IXPs are integral parts of Internet infrastructure. Ensuring network interconnection[14] is key to Internet infrastructure resilience.

IXPs allows the networks to exchange Internet traffic locally, rather than over international networks. They reduce network delays, and lower Internet-access costs for end-users by decreasing ISP operating costs.[15] [16] However, while IXPs help with network interconnection by dealing with traffic more efficiently and locally, they cannot fix a lack of alternative physical paths for data to travel. This is why both are important. In addition to IXPs, a diversity and richness of international connectivity is also essential.

**What Are IXPs?**
An Internet Exchange Point (IXP) is a physical location where different IP networks – including ISPs, content providers and Content Distribution Networks (CDN), governments, and research networks – connect and exchange local traffic with each other over a shared platform. They form an integral part of the Internet ecosystem.

More info:
https://www.internetsociety.org/issues/ixps/

*Routing security*[17]

Internet Protocol (IP) routing makes the Internet work by ensuring that data-packets go where they are meant to when transiting between carriers. Routing incidents[18] - whether through configuration errors or malicious attacks - can create real economic harm by making key services unreachable. They can also divert data packets through malicious networks, providing an opportunity to spy on them. Incidents like route hijacking, route leaks, IP address spoofing are global in scale, with one operator's routing problems cascading to impact others.

[12] https://gulfnews.com/technology/uae-is-second-most-targeted-country-in-middle-east-and-africa-for-ransomware-1.2020895
[13] https://www.cybersecurity-review.com/news-may-2018/phishing-spy-campaign-targets-top-mideast-officials/
[14] https://www.internetsociety.org/policybriefs/internetinterconnection/
[15] https://www.internetsociety.org/policybriefs/ixps/
[16] https://www.internetsociety.org/resources/doc/2018/routing-security-for-policymakers/
[17] https://www.internetsociety.org/resources/doc/2018/routing-security-for-policymakers/
[18] https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/

Mutually Agreed Norms for Routing Security (MANRS[19]) is a global initiative, supported by the Internet Society, provides crucial fixes to reduce the most common routing threats. Versions of MANRS for network operators and IXPs are available and are described in more detail in Annex III.

Arab context: The Arab states still have a relatively small number of IXPs, and it is not clear that all are operational. There are currently fifteen IXPs in the Arab states, spread out amongst nine countries.[20] Eight of these appear operational; in Egypt, Kuwait, Lebanon, Palestine, Saudi Arabia, and the United Arab Emirates. There is considerable scope to increase the number and reach of IXPs to optimise network interconnectedness.

Regarding routing security, there were 14,000 routing incidents globally in 2017[21], but the Arab states are not currently thought to have fallen victim to a major, concerted attack. However, as state actors in other regions appear increasingly likely to use intentional route-hijacking to maliciously re-route traffic in order to spy on it, the risk of such an attack in the Arab region may increase. The regional risk will be decreased if significant numbers of network operators adopt MANRS.

## Communication Infrastructure

Communications infrastructure means the essential physical assets needed to operate the Internet; cabling and linking (Wireless; microwave, cable, satellite. Wired; fibre, copper, broadband), buildings (facilities including data-centres or landing points for undersea cables) and also power supply, cooling systems and physical security.

Arab context: There seems to be lower "path resilience" than what is needed for resilient regional networks, i.e. if there is only one physical path for traffic to enter and leave the country or region, a single point of failure exists. Undersea cable accidents have caused breakdowns in connectivity of Internet infrastructure– region-wide for example, the 2013 cable-cutting near Alexandria, Egypt, which caused Internet slowdowns around the Middle East.[22] This type of incident shows the need for path resilience for traffic-routing, so that traffic is not concentrated in a small number of regional choke-points. The Internet is a 'network of networks', so focusing purely on national network resilience will not ensure ongoing connectivity; regional Internet resilience needs to be the goal. Robust Internet infrastructure means having sufficient physical paths for Internet traffic to go to and from other countries in the region and globally, especially when a path is no longer available due to natural disaster, human error or attack.

## Information

Information includes data about systems (for example, inventories of software, hardware, infrastructure), network topology (how the network is mapped), system configuration and operational information.

Arab context: Information-sharing and reporting of data-breaches are comparatively low and there are unusually long times taken to remediate them. A low level of overall breach notification means breaches throughout ICT systems tend to go undetected.[23]

[19] https://www.manrs.org/

[20] "Middle East & North Africa Internet Infrastructure" report to be published, December 2019: https://www.internetsociety.org/regions/middle-east/

[21] https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/

[22] https://gigaom.com/2013/03/27/undersea-cable-cut-near-egypt-slows-down-internet-in-africa-middle-east-south-asia/

[23] http://www.securitymea.com/2019/07/01/darkmatter-group-releases-mena-cybersecurity-report/

## Human Resources

Human resources comprises the people considered as an asset to the security of Internet infrastructure, including administrators, operators, support teams, developers, managers, auditors and end-users. People - and their skills and capabilities, formal and informal networks, and sense of empowerment to act as needed during security incidents - are an essential part of Internet infrastructure. Well-trained and effective people improve the security of the systems they operate and use. Key factors that need to be pro-actively developed are competence, understanding and support from management, staff's discipline to follow procedures (especially senior staff), and the trustworthiness of all. Related to human resources is the set of governance arrangements, both formal and informal, that structure Internet infrastructure security. This includes clear reporting lines and responsibilities, incentives for collaboration, and encouragement for effective and appropriate information-sharing through CSIRTs and other parts of the local security community.

Arab context: As in other regions, there is a security skills-gap.[24] Arab countries tend to have lower numbers of accredited cybersecurity professionals and in some countries these skills may be concentrated in expatriate workers.[25] There are different needs for skills and experience at entry-level and in more senior roles, suggesting a need for more cybersecurity education at second and third levels and in ongoing development. More specialist knowledge and training can also be delivered in ongoing professional training related to the activities of CSIRTS and other sectoral initiatives.

# 3 Internet Infrastructure Security Principles

This section sets out the basic principles needed to for securing Internet infrastructure. These general principles were adapted from guidelines developed by the Internet Society based on the expertise of its members, and current best practice around the world26. They also draw on recommendations and best practice from organizations including the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), the International Telecommunication Union (ITU), the US National Institute of Standards and Technology (NIST), the European Union Agency for Network Information and Security (ENISA), the African Union,27 and the Organisation for Economic Cooperation and Development (OECD).28 The principles have been adapted in consultation with experts and officials in the Arab states.

## Awareness

Stakeholders in both the public and private sectors need to understand their own security risks, as well as how they and others in the Internet infrastructure ecosystem are impacted by these risks. Everyone responsible for part of the Internet infrastructure needs to recognize their risks and manage them within their roles, to minimize the impact on themselves and others in the Arab Internet infrastructure ecosystem.

[24] https://thearabweekly.com/skills-gap-exacerbates-cybersecurity-problem-middle-east-faces-threats

[25] https://www.fircroft.com/blogs/security-in-the-digital-age-a-report-on-the-middle-east-cyber-72474105124

[26] Internet Infrastructure Security Guidelines for Africa; A joint initiative of the Internet Society and the Commission of the African Union; https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/

[27] African Union Convention on Cyber Security and Personal Data Protection; https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[28] Adapted from the Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document.

### Responsibility

Each stakeholder should take responsibility for the management of security risks within their respective roles and organizations. Due to the fundamentally interdependent and interconnected nature of the Internet, each organization should consider the potential impacts of their actions or inaction on other stakeholders.

### Collaboration

All stakeholders, including those across borders, must be included in an ongoing cybersecurity dialogue to effectively counter new and persistent threats. This includes both formal and informal consultations and also the establishment of collaborative relationships between the public and private sectors. The security of Internet infrastructure cannot be achieved by any one organization alone, and a "top-down control" approach will not achieve the needed information flows and cooperation that are essential to regional resilience.

### Fundamental Rights and Internet Properties

All stakeholders' actions to manage security risks should adhere to fundamental rights, be transparent, and not infringe upon the Internet properties of voluntary collaboration, open standards, reusable technology building blocks, integrity, permission-free innovation and global reach.[29]

Policies and strategies should include consideration of their impact on the underlying architecture of the Internet and ensure that they do not negatively impact the openness, innovation and global reach of the Internet.

# 4 Current Developments in the Arab States

Many of the Arab states are tackling Internet infrastructure security in different ways, including national strategies and the creation of Computer Security Incident Response Teams (CSIRTs). National and regional capabilities and approaches are still developing; not all countries have adopted and implemented national cybersecurity strategies, and, as an overall, CSIRTs are not yet maximizing opportunities for collaboration

The essential next phase of securing Internet infrastructure will be to expand the current largely state-centred focus to a fully collaborative and cooperative approach. But while much needs to be done, several countries have seen "quick wins" for their national resilience from the activities of collaborative incident response centres.

## 4.1 National Cyber Security Strategies

Several Arab states - Oman, Jordan, the United Arab Emirates and Egypt - have implemented pro-active cyber security strategies to address their threat landscape in a pro-active way.

**Oman** places 4th globally, in the International Telecommunication Union's Global 2017 Cybersecurity Index (GCI), and 16th in 2018[30]. The GCI measures survey responses across the 'pillars' of legal, technical, organizational, capacity-building and cooperation. (The GCI also measures Saudi Arabia, Qatar, Egypt and the United Arab Emirates as having a 'high' level of commitment to cybersecurity.) With its hosting of the

[29] https://www.internetsociety.org/internet-invariants-what-really-matters

[30] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

ITU Arab Regional Cybersecurity Centre (ITU-ARCC), Oman also supports other countries, in the region and further afield.

**Jordan** completed a five-year National Information and Cybersecurity Strategy (2012 – 2017)[31], including the establishment in 2013 of a National Computer Emergency Response Team. Jordan's second five-year strategy[32] began in 2018 to address the rapid development of new technologies - including automation - and the increasing threat and number of cyber-attacks across both the public and private sectors.

The **United Arab Emirates'** National Cyber-Security Strategy[33] aims to create a safe and strong cyber-infrastructure for citizens and businesses. The updated version of the strategy was launched in 2019 by Telecommunications Regulatory Authority (TRA), the entity responsible for the ICT sector and digital transformation in the country. The strategy is based on five pillars and sixty initiatives aiming to mobilize the whole cyber security ecosystem in the UAE. The new strategy aims to increase citizens' confidence in the digital world, encourage innovation and entrepreneurship in cybersecurity, enable SMEs to protect themselves against the most common cyber-attacks, protect critical information infrastructure assets and "build a world-class cybersecurity workforce in the UAE."[34]

**Egypt** established a Supreme Council for Cybersecurity, composed of government agency representatives, in 2015. The national cybersecurity strategy (2018) was developed in view of the strategic objectives that led to the creation of the Egyptian Supreme Cybersecurity Council (ESCC), reporting to the Cabinet of Ministers, and chaired by the Minister of Communications and Information Technology. It includes six strategic program areas. One program, a legislative framework to "secure cyberspace, combat cybercrimes and protect privacy, and digital identity", is to be implemented in cooperation with all stakeholders, including government, private sector, academia and civil society. A further program is to develop CSIRTs in critical sectors. Other programs focus on developing skills and capacity in cybersecurity and supporting research and development.

## 4.2 Computer Security Incident Response Teams (CSIRT)

A Computer Security Incident Response Team (CSIRT) – also sometimes known as a CERT (Computer Emergency Response Team or Computer Emergency Readiness Team) - is an organization or community of experts that receives, reviews, and responds to computer security incidents. It may be geographical or sector-specific, and led by the public and/or private sector. CSIRTs provide a critical knowledge-sharing function to ensure security. Many Arab states operate CSIRTs / CERTs. Some also run more broadly-based cybersecurity coordination centres that do outreach, ongoing training, accreditation of cybersecurity experts including 'white hat' security researchers, and other activities to increase capacity and develop and deepen stakeholder relationships.

Tunisia was one of the first Arab states to establish a CSIRT in 2007, based on the Information Safety Law No. 5 of 2004. The law also makes provision for responses to attacks or breaches involving government institutions, setting out the operational relationship between the National Agency for Information Safety and any ministries under attack.[35]

[31] http://nitc.gov.jo/PDF/NIACSS.pdf

[32] http://moict.gov.jo/uploads/Public-Consultations/NCSS-DRAFT.pdf

[33] https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/national-cybersecurity-strategy-2019

[34] Ibid.

[35] https://legislation-securite.tn/fr/node/44031

CSIRTs have also been established in the United Arab Emirates, Tunisia, Egypt, Sudan, Oman and Saudi Arabia, where they work to improve overall information security nationally, protect the IT infrastructure from cyber-risks, threats and attacks, and also provide direct technical support for government agencies. (The ITU has carried out assessments of readiness for the establishment of a CSIRT in Comoros, Djibouti, Mauritania, Palestine.36)However, while the established CSIRTs often do excellent work, they tend to be under-resourced financially and in terms of equipment, people, skills and lack the empowerment to form the collaborative relationships and networks.

Despite the challenges they face, CSIRTs have already played a key role in protecting Internet infrastructure in the region:

- **Oman** established its own CSIRT in 2010 and hosts the ITU Regional Centre for Electronic Security for the Arab Region**,** which aims to provide services and initiatives to the region to improve electronic security through regional cooperation.
- **Jordan**'s JO-CERT is an overall national CSIRT that has also established a new centre for cybersecurity expertise alongside its operational role. Jordan also has an armed forces organization, JAF-CERT, and plans to establish a banking / financial services CERT in the future. Jordan is also working to establish a national platform for information or threat intelligence-sharing (i.e. an Information Sharing and Analysis Centre – ISAC).
- The **United Arab Emirates** Computer Emergency Response Team (aeCERT) aims to protect the IT infrastructure. It disseminates information about threats, vulnerabilities and cybersecurity incidents. aeCERT provides services to government entities, including incident response, digital forensics, vulnerability assessment, penetration testing, awareness campaigns and sessions, and phishing assessments.[37]
- In **Egypt**, the EG-Cert is up and running, and the 2017-2021 National Cybersecurity Strategy include,s as a key program, an integrated national system to protect cyberspace and secure ICT infrastructure with CERTs in critical sectors at the national level, "based on the pioneering experience of the ICT sector."[38]
- **Bahrain**'s government CSIRT takes the lead in securing government networks. Bahrain plans to establish a sectoral CSIRT in 2020.

**How CSIRTs Work**

Since the late 1980s, the concept of CSIRTs has spread around the world as a key model to deal with incidents such as malware, breaches, DDOS attacks and other threats. Day to day, CSIRTs typically work with other organizations – e.g. banks, universities, infrastructure providers and other private sector bodies – to share information and expertise, develop capacity and build relationships to manage ongoing threats and prepare for incident response.

During critical incidents, a CSIRT is "generally the focal point for coordinating and supporting incident response."[1] Being able to exchange information can limit the amount, type, duration, and impact of attacks.[2]

The CSIRT model is based on collaboration and openness. Rapidly sharing information about vulnerabilities, malware and attacks is essential for them to work effectively. When a serious or widespread attack or threat appears, the CSIRT must also be able to spring into action, relying on other organizations nationally and CSIRTs in other countries in the region and globally in order to get information and assistance. These relationships take time and care to build, as they are based on knowledge and trust. If countries do not put the resources into building both skills *and* relationships, they are likely to be less effective in responding to critical incidents.

1 https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams
2 https://www.researchgate.net/publication/319645577_Cyber_Security_Capacity_Does_it_Matter

[36] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

[37] https://www.tra.gov.ae/aecert

[38] http://www.mcit.gov.eg/Upcont/Documents/Publications_12122018000_EN_National_Cybersecurity_Strategy_2017_2021.pdf

- Teams from a range of Arab countries have achieved membership of the global Forum of Incident Response and Security Teams (FIRST),[39] an international group of public and private sector CSIRT teams set up to share information, knowledge and best practice and deal with incident response; **Morocco, Tunisia, Egypt, Saudi Arabia, Oman**, and the **United Arab Emirates.**

Compared to other regions, Arab state CSIRTs tend to operate a more state-led, 'top-down control' approach. With this approach, governments may face challenges to align incentives with other stakeholders, particularly on information-sharing and vulnerability-disclosure. Some government-controlled CSIRTs are aligned with national intelligence priorities and may find it challenging to build trust and coordinate with government counterparts in other countries. Nonetheless, there is considerable interest in sharing experience and expertise, particularly amongst the Gulf States. Our consultations showed support for increased regional cooperation between CSIRTs / cybersecurity coordination centres, including the concept of a real-time threat intelligence platform for Arab countries.

Several Arab governments have developed different ways to engage with "white hat" security researchers (also called "ethical hackers") who do penetration or other forms of system or network testing aimed at ensuring the security of an organization's information systems.[40] These governments are working to harness and develop people's available skills and experience in a way that incentivizes collaboration and reduces risk. In this emerging area, participants in our regional workshops shared the approaches they have used;

- **Oman** has held cyber talent challenges and is developing a directory of white hat hackers or 'cyber ambassadors'
- **Tunisia** is licensing cybersecurity service providers and has held hackathons or organized penetration testing events for infrastructure
- **Jordan** has passed a law to improve trust by licensing cyber security services.

Other suggestions included one to establish a legal framework to facilitate researcher collaboration with CSIRTs/CERTS and law enforcement agencies on vulnerability testing, and another to expand the role of national Internet Society chapters[41] or global Special Interest Groups[42] to attracting volunteers for cyber security activities and coordinating with CERTs.

This is a complex and sometimes ambiguous area where the intent behind vulnerability research and penetration testing is not always clear. Several governments are working to identify or accredit ethical security researchers and to avoid disincentivizing useful activities that build overall resilience and a local skill-base. More than anything, relationships of trust and flexibility are important, so care should be taken not to stifle cooperation with an overly legal system for collaboration.

## 4.3 National and Regional Communication and Collaboration

National communication and collaboration cybersecurity initiatives are still at a relatively early stage in most Arab States. This matches many other regions of the world. Globally, fewer than half of the world's countries have "a public-private partnership cooperative arrangement".[43] The ITU describes the multistakeholder approach to cybersecurity as including initiatives *"with inputs from all sectors and*

[39] https://www.first.org/

[40] https://en.wikipedia.org/wiki/White_hat_(computer_security)

[41] https://www.internetsociety.org/chapters/

[42] https://www.internetsociety.org/sigs

[43] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

*disciplines (including bilateral and multilateral agreements, participation of international fora/associations, public-private partnerships, inter-agency partnerships, best practice".*[44]

There is a growing trend in the Arab states to develop more collaborative partnerships at the national level – for example, in the recent emergence of sectoral CSIRTs. Regional communication and collaboration efforts are increasing, and there is a clear drive to deepen regional cooperation where appropriate and productive.

# 5 Recommendations

Governments should bring their approach to Internet infrastructure security up to date by focusing on the underlying purpose of Internet security; that security is no longer the end-goal but a means to facilitate overall social and economic goals. Security today is less about building walls around infrastructure, and now recognises its role in facilitating a global, interconnected and interdependent global digital economy. Maintaining national and regional connectivity is a key goal.

As the Internet is a 'network of networks', focusing purely on national network resilience will not ensure ongoing connectivity; regional Internet resilience needs to be the goal. To achieve this, governments need to participate and coordinate regionally.

### Summary Table of Recommendations

| National Recommendations | Regional Recommendations |
|---|---|
| Governments should foster an open, collaborative and resilient Internet security ecosystem that includes:<br>• Identifying and protecting critical information infrastructure<br>• Improving Internet infrastructure security by facilitating deployment of security standards and best practices<br>• Improving Internet infrastructure resilience through better network interconnection<br>• Facilitating information exchange and relationship-building across stakeholders<br>• Establishing and strengthening national-level CSIRTs<br>• Using public institutions to lead by example<br>Identifying and addressing legal barriers to information-sharing (including supporting 'white hat' security researchers) and research on security vulnerabilities, incidents and threats<br>Working to harness and develop ethical hacking skills with talent challenges, hackathons, and local communities of white hat hackers or appropriate licensing of cybersecurity service providers | Governments should work with all stakeholders to strengthen regional collaboration:<br>• Establish a regional group of security experts from government, business, technical, academic and civil society to provide non-binding guidance to the region on Internet security infrastructure issues as needed.<br>• Participate in and deepen existing communication and coordination cybersecurity initiatives, including consideration of whether to establish a regional threat intelligence-sharing platform<br>• Pool CSIRT/CERT resources where possible, for example, coordinating and sharing training courses between CSIRTs – to increase knowledge and experience and to build cross-border relationships between professionals that build trust for further collaboration<br>• Increase path and routing resilience for Internet traffic on a regional, 'network of networks' basis to increase network exit points and reduce physical chokepoints or "single points of failure". |

[44] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

## 5.1 National Recommendations

Governments should foster an environment that emphasizes an open, collaborative and resilient Internet security ecosystem. Governments and other stakeholders should empower organizations and individuals through information sharing, promoting best practices, and leading by example.

Alongside their role in facilitating information-sharing and promoting best practices, governments hold the unique position of setting policy and showing leadership in the Internet infrastructure ecosystem. Governments should champion awareness and accountability, consider the potential impact of new policies on all stakeholders and involve them in their development. Policies and any laws enacted by governments should adhere to the four essential principles of awareness, responsibility, cooperation, and preservation fundamental rights and Internet properties.

### 5.1.1 Identify and Protect Critical Information Infrastructure

All stakeholders should work together to accurately identify and classify the interconnected systems and networks needed to ensure the well-being of citizens, provision of essential services and the effective functioning of government and the economy. Accurate identification and classification of systems is the foundation of successful security risk management. It ensures that appropriate security measures can be focused on critical services and information infrastructure, and prevents the use of resources spending in non-critical areas.

All stakeholders should prioritize critical information infrastructure, conduct risk assessments and implement appropriate security policies and practices, while maintaining functionality.

Threat-modelling can also be a useful way to identify and protect critical information infrastructure. It looks at infrastructure from an attacker's point of view to determine the threat vectors likely to be used and their probable targets. More detailed guidance for network operators is available in Annex III of this document.

### 5.1.2 Improve Internet infrastructure resilience by facilitating deployment of security standards and best practices

In an interconnected world with dependencies spanning multiple networks, nations and continents, it is vital that all participants strive towards best practices in Internet infrastructure security. The guidance for network operators in Annex III may also be applicable to both public and private sector organizations responsible for parts of critical Information infrastructure, for example, operators of country code Top Level Domains (ccTLDs) or large government networks.

Annex III of this document sets out more detailed guidelines for network operators, including the implementation of protocols and practices for routing accuracy, DNS and email security. It also includes links to further resources on how network operators and IXPs can implement Mutually Agreed Norms on Routing Security (MANRS).

### 5.1.3 Improve Internet infrastructure resilience through better network interconnection

Governments should promote the use of Internet Exchange Points (IXPs) nationally, and increase cooperation and connectivity between different Arab networks regionally, to improve interconnection including international links. Network operators and IXPs should also implement Mutually Agreed Norms for Routing Security[45] This will help to increase routing and resilience of Internet data.

### 5.1.4 Facilitate Information Exchange and Relationship-Building

Recognizing that security tends to be handled in a more centralized, state-led way in these countries, there is still scope to promote information-sharing. Improving breach-reporting and information-sharing will improve all stakeholders' ability to deal with incident prevention and response.

This requires improving trust between stakeholders, particularly via public-private partnerships. Trust can be built through frequent formal and informal contact, identifying and working towards shared goals, and ensuring the technical credibility of institutions and individuals.46 Trust also needs to be built on the recognition that other stakeholders are valued partners with their own priorities and expertise.

This facilitation can grow from the specific trust relationships needed for effective disclosure, but can also involve a wider context of consultation and dialogue between government, national CSIRTs, civil society, academia, the technical community, and private sector. These conversations – both formal and informal – can identify areas where action is needed on a national level, for example, new training programs to alleviate a capacity gap in a specific security area, or adopting an up to date security practice within government agencies.

### 5.1.5 Establish and Strengthen National Level Computer Security Incident

**Response Teams (CSIRTs)**

CSIRTs are vital in addressing Internet infrastructure security issues. They perform an important function in identifying security incidents, helping organizations protect themselves against cyber-attacks, and in recovery. The frequency and gravity of cyber-threats necessitates effective watching, warning and incident response capabilities.

Governments should work with other stakeholders, including the technical community

to establish CSIRTs where none exist, and to support CSIRTs that work collaboratively to promote awareness, responsibility, cooperation and fundamental rights and Internet properties.

Governments can also encourage the operation of CSIRTs to:

- Ensure incentives are aligned to maximize information-sharing and increase transparency regarding known vulnerabilities and cyber-attacks
- Where CSIRTs are centralized and government-run, increase their ability to disseminate knowledge, build collaborative relationships and open up participation from regional experts
- Ensure CSIRTs are sufficiently resourced to support gathering and analysing of threat intelligence and disseminating actionable information
- Ensure government institutions lead by example, using CSIRTs for information-sharing and capacity-building

[45] https://www.internetsociety.org/issues/manrs/

[46] https://www.researchgate.net/publication/319645577_Cyber_Security_Capacity_Does_it_Matter

### 5.1.6 Use Public Institutions to Lead by Example in Cybersecurity

Governments, as owners and operators of information systems and networks, can lead by example by adopting best practices, using security technologies, and through their procurement processes. Governments should also consider using tools such as economic incentives, encouraging industry to pro-actively improve cybersecurity, and empowering citizens to demand better security solutions. Sometimes these solutions can be as or more effective than laws.

Governments should also prioritize Internet infrastructure and maintaining connectivity in national strategies for security, keeping in mind that the overall objective of security is to serve social and economic prosperity. Governments should actively promote the use of security standards and best practices in their own infrastructure, by their agencies, and by third-party suppliers of government services.

Governments can also use their budgets to ensure that appropriate resources, including budget and staff, are allocated to governmental departments and agencies to operate and secure their systems.

### 5.1.7 Identify and address legal barriers to information-sharing (including 'white hat' security researchers), the implementation of security technologies and research on vulnerabilities, incidents and threats.

Legal barriers can impede security researchers from disclosing information about vulnerabilities. "White hat" or ethical hackers, who perform penetration and other system and network testing from outside an organization, may worry that disclosing identified vulnerabilities, routing security incidents or threats could place them in legal jeopardy. Governments should introduce better acceptance and support for "white hat" or ethical hackers and security researchers. They can do this by:

- Identifying and eliminating legal barriers to information and vulnerability-sharing.
- Working to harness and develop people's available skills in a way that incentivizes collaboration, for example, with cyber talent challenges or hackathons, communities of white hat hackers.
- Considering frameworks for researchers to collaborate with CSIRTs on vulnerability testing.

## 5.2 Regional Recommendations

### 5.2.1 Participate in and deepen existing communication and coordination cybersecurity initiatives

Regional interactions and initiatives that promote cooperation between states are a key way to foster an overall collaborative approach that benefits everyone.[47] Governments should pro-actively participate in regional and international fora for cybersecurity cooperation, focusing efforts on inclusive collaboration, coordination and information-sharing among all stakeholders that supports the Internet's fundamental properties.

In addition to coordinating with the ITU Regional Centre for Electronic Security for the Arab Region and Regional Cyber Security Summit for the Arab States, governments and other stakeholders should consider participating in global initiatives. The following fora can help them deepen and share knowledge about Internet infrastructure security, and build relationships across sectors and borders.

[47] https://www.oecd-ilibrary.org/science-and-technology/the-promotion-of-a-culture-of-security-for-information-systems-and-networks-in-oecd-countries_232017148827

These relationships and the up to date flow of knowledge and best practice they bring could be essential in dealing with critical incidents in the future:

- Global Forum on Cyber Expertise (GFCE)
- Global Commission on the Stability of Cyberspace (GCSC)
- Global Cyber Security Capacity Centre, Oxford (GCSCC)

Further, governments should engage all stakeholders, including across borders, to determine if it is useful and practical to establish greater regional threat intelligence-sharing that builds on some existing bi-lateral relationships to share information about threats and vulnerabilities in real-time.

### 5.2.2 Pool CSIRT resources regionally

Where possible, CSIRTs across the region should pool their resources. For example, they could coordinate or even and make training courses accessible to other CSIRTs. This would increase knowledge and experience across the region and also build cross-border relationships between professionals that develop relationships and trust for further collaboration.

### Increase regional path resilience for Internet traffic

The Internet is a 'network of networks', so focusing purely on national network resilience will not ensure ongoing connectivity; regional Internet resilience needs to be the goal. Undersea cable accidents have caused breakdowns in connectivity of Internet infrastructure region-wide.[48] This shows the need for path resilience for traffic-routing, so traffic is not concentrated into a small number of regional bottle-necks (or single points of failure).

Governments should work with other stakeholders on a regional, 'network of networks' basis to increase rich and diverse connectivity of networks, both nationally and internationally, to reduce single points of failure and bottlenecks.

All stakeholders should also work towards more cross-border cooperation between network operators and IXPs across the Arab states to coordinate, share knowledge and respond to incidents.

# 6 Acknowledgements

These guidelines were developed in consultation with cybersecurity experts in the Arab states and beyond, and members and staff of the Internet Society, including chapters of the organization in the region who reviewed the guidelines.

The Internet Society particularly wishes to thank the following institutions and their staff for their support of our preparatory and consultative process;

- Chatham House, the Royal Institute of International Affairs, for hosting a consultation workshop, May, 2019
- The Kingdom of Saudi Arabia, for hosting a consultation workshop, June 2019
- The State of Kuwait, for hosting a consultation workshop, September, 2019

[48] https://gigaom.com/2013/03/27/undersea-cable-cut-near-egypt-slows-down-internet-in-africa-middle-east-south-asia/

- The Sultanate of Oman, for hosting a consultation workshop, November, 2019

The Internet Society is grateful to regional experts for their active participation in this process and valuable contributions, including the following institutions:

- The Ministry of Digital Economy and Entrepreneurship and the Telecommunications Regulation Authority of the Hashemite Kingdom of Jordan
- The Telecommunications Regulatory Authority of the United Arab Emirates
- The Telecommunications Regulatory Authority of the Sultanate of Oman
- The Telecommunications Regulation Authority of Bahrain
- The National Telecom Regulatory Authority of the Arab Republic of Egypt
- The Communication and Information Technology Regulatory Authority of the State of Kuwait
    - The Ministry of Telecom and Information Technology of the State of Palestine
    - The Telecommunication and Postal Regulatory Authority of the Republic of the Sudan
    - The Internet Society Sudan Chapter
    - The Tunisian Internet Agency of the Republic of Tunisia

We wish to acknowledge the invaluable contributions of Internet Society staff members Nermine El Saadany, Christine Runnegar, Ryan Polk, Sally Wentworth, Jane Coffin, Olaf Kolkman, Salam Yamout, Max Stucchi and Andrei Robachevsky for their leadership, input and advice, and Maria Farrell (consultant) who edited these guidelines.

# Annex I: Methodology and Resources

These guidelines are adapted to suit the specific needs of the Arab states, drawing best practice and advice from frameworks and instruments including;

- Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document (2015)[49]
- National Cyber-Security Strategy Good Practice Guide, European Union.[50]
- African Union Convention on Cyber-Security and Personal Data Protection (2014) [51]
- Internet Infrastructure Security Guidelines for Africa; A joint initiative of the Internet Society and the Commission of the African Union[52]

Internet Society resources which may be useful to policymakers include:

- Collaborative Security: An approach to tackling Internet Security issues[53]
- Policy Brief: Botnets (2015)[54]
- Routing Security for Policymakers[55]
- An Overview of Internet Content-Blocking[56]
- Policy Brief: Internet Exchange Points (IXPs) (2015)[57]

# Annex II: Internet and Security-Related Terms

These definitions do not form a complete glossary, nor are they the authoritative definitions. They are intended to provide a simple introduction to the terms.

## Attacks

Attackers may use a variety of tools, scripts, and programs to launch attacks against networks and network devices, and to deceive or otherwise compromise staff or vendors with access to the network – whether on-site or remotely. Typically, the network devices under attack are the endpoints, such as servers and desktop computers. A cyber-attack occurs if an attacker successfully breaches security controls.

[49] http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf

[50] https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[51] https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf

[52] https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/

[53] https://www.internetsociety.org/collaborativesecurity/approach/

[54] https://www.internetsociety.org/policybriefs/botnets/

[55] https://www.internetsociety.org/resources/doc/2018/routing-security-for-policymakers/

[56] https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/ and Arabic version: https://www.internetsociety.org/wp-content/uploads/2017/03/ISOC-ContentBlockingOverview_ar.pdf

[57] https://www.internetsociety.org/policybriefs/ixps/

## Breaches

In the context of networks, "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision"[58] of an electronic communications service.

## Collaborative Security Approach

The collaborative security approach to Internet security recognizes that people are what ultimately hold the Internet together. The Internet's development has been based on voluntary cooperation and collaboration. Cooperation and collaboration remain the essential factors for its prosperity and potential. The approach emphasizes five principles:

- preserving opportunities and building confidence;
- collective responsibility;
- security solutions fully integrated with rights and the open Internet;
- security solutions grounded in experience, developed by consensus and evolutionary in outlook; and
- targeting the point of maximum impact – think globally, act locally.[59]

## Computer Security Incident Response Team (CSIRT)

An organization or community of experts that receives, reviews, and responds to computer security incidents. They may be geographically or sector specific, and led by the public and/or private sector. CSIRTs provide a critical knowledge sharing function to ensure security.

## Critical Information Infrastructure

Interconnected systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, the provision of essential services, or the effective functioning of government or economy.

## Distributed Denial of Service (DDoS) Attacks

A DDoS attack "is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources".[60]

## Domain Name System (DNS):

"DNS is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols."[61]

[58] https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/.

[59] https://www.internetsociety.org/collaborativesecurity/

[60] http://www.digitalattackmap.com/understanding-ddos/

[61] https://en.wikipedia.org/wiki/Domain_Name_System

## Fundamental Properties of the Internet

“Characteristics which have enabled the Internet to serve as a platform for seemingly limitless innovation, outline not only its technology, but also its shape in terms of global impact and social structures”.[62]

These identified characteristics are;

- voluntary collaboration,
- open standards,
- reusable technological building blocks,
- integrity,
- permission-free innovation, and
- global reach.

## Internet Exchange Point (IXP)

A system that allows many Internet-based networks to exchange traffic with each other at a common meeting point, thus eliminating the need to build separate bilateral links with each local network.

## Internet Infrastructure

The elements which make up and enable the movement of data across an interconnected network of networks. These elements include protocols and services, software and hardware, network interconnection, communication infrastructure, information, and human resources.

## Internet Service Provider (ISP)

A company or organization that provides individuals, organizations, enterprises and others with access to the Internet. Aside from connecting users, ISPs often provide other services such as email and hosting of websites for their customers.

## Routing

Routing determines how traffic will travel from one point in the network(s) to another. Network nodes that make routing decisions are called routers. Reachability information (i.e. whether a particular network can be reached through a node) is exchanged among the Internet routers. The two types of protocols used to exchange this information are Interior Gateway Protocol used between the routers inside a network (such as OSPF, IS-IS or RIP) and exterior gateway protocol used between networks, or autonomous systems (AS), which is Border Gateway Protocol (BGP). One of the vulnerabilities of BGP is that it does not provide means to check the validity of the information exchanged.

Such validation requires use of additional tools and practices.

[62] https://www.internetsociety.org/internet-invariants-what-really-matters

### Stakeholders

The individuals, groups, organizations, entities or communities which have an interest or stake in the Internet. Stakeholders include governments, the private sector, civil society, academia, and the technical community.

# Annex III: Guidance for Network Operators

This document has largely focused on steps governments should take. As a significant amount of Internet infrastructure is typically in private sector hands, in the telecoms industry, the following guidance focuses on what network operators need to do.

## 1 ISP/Operator Level

Network operators have a direct role in securing Internet infrastructure as they operate the networks in Africa. A security weakness in one operator's network not only affects that network, but potentially other networks in Africa, and those across the world.

## 1.1 Establish Baseline Security

Addressing Internet infrastructure security challenges requires collaboration and commitment from all stakeholders. In an interconnected world with dependencies spanning multiple networks, nations and continents, it is very important that all participants adhere to at least a minimum level of security – a baseline level which many will immediately surpass, and from which others can build.

### Routing and Domain Name System Security

Network operators should prevent propagation of incorrect routing information; prevent traffic with spoofed source IP addresses; facilitate global operational communication and coordination between network operators; and facilitate validation of routing information on a global scale. IP spoofing, or source address forgery, is often used in denial of service attacks to make defensive filtering more difficult.

Network operators should enable DNSSEC[63] validation on their DNS resolvers to ensure the integrity and authenticity of DNS transactions. DNS registry operators, operators of authoritative DNS servers and domain registrars should support DNSSEC and implement common security practices, such as access control and vulnerability and patch management.

Network operators should also integrate other best current practices related to routing security and resilience in their network management processes. A global initiative, MANRS, the Mutually Agreed Norms for Routing Security[64], defines a concise package of minimum but critical measures to ensure the resilience and security of the global routing system. MANRS was created by members of the network operator community with support from ISOC. MANRS has simple steps for network operators to dramatically improve Internet security and reliability. MANRS was initially designed for network operators, but Internet Exchange Points (IXPs) are important partners with a separate set of MANRS Actions. For more information, visit https://www.manrs.org/.

[63] https://www.internetsociety.org/deploy360/dnssec/basics/

[64] https://www.manrs.org

### Network Security

Securing one's network is necessary to protect the network and others in the Internet ecosystem. This includes filtering spoofed traffic and volumetric attack traffic, both incoming and outgoing, from their networks. Outgoing spoofed and attack traffic may lead to IP address reputation problems for the originating network, but will often lead to more direct negative impacts on other networks in the Internet ecosystem.

ISOC's Anti-Spam Toolkit[16] provides best practices for policymakers, network operators, and users to better secure their networks from the threat of spam. The Toolkit also provides links to outside resources on spam and combating unwanted traffic. M3AAWG's Anti-bot Code of Conduct[17] for Internet service providers advises ISPs to engage in education, detection, notification, remediation, and collaboration. The Code of Conduct promotes the essential principles of awareness, responsibility, cooperation, and upholding the fundamental rights and Internet properties.

### Essential Security Practices

Secure protocols should be used in products and services supporting Internet infrastructure. For instance, TLS[65] (transport layer security) is a cryptographic protocol that should be employed to protect web services. TLS encrypts data exchanged in an HTTP transaction and cryptographically identifies one or more of the parties engaged in a transaction. Privacy and identity are fundamental elements of secure Internet infrastructure.

Operators of e-mail services should deploy appropriate email security standards and practices such as DKIM, SPF and DMARC.[66]

Operators must also ensure software critical to Internet infrastructure is being effectively managed for security vulnerabilities. Only software that is being maintained by a vendor or an open source community should be deployed in Internet infrastructure. Operators should employ a patching policy that prioritizes the mitigation of software vulnerabilities, despite the inherent risk to up-time. Operators may also build a software vulnerability management program granting responsibility for the continued mitigation of software vulnerabilities to an individual or institution. A lack of institutional accountability for software vulnerability management is a common reason why many organizations fail to patch appropriately.

## 1.2 Establish and Maintain Cooperation and Collaboration

Beyond their participation in the national multistakeholder structures outlined in Section 3.2.2, ISPs and network operators have a responsibility to coordinate and collaborate with one another, their customer organizations, and other stakeholders. ISPs and network operators should:

- Encourage cooperation and collaboration with customer organizations, local and regional governments, and regulators in preventing, detecting and mitigating routing incidents
- Facilitate global operational communication and coordination between network operators
- Actively participate in ISP associations such as national and regional network operator groups and fora

[65] https://www.internetsociety.org/deploy360/tls/basics/

[66] https://www.internetsociety.org/resources/ota/2017/email-authentication-dmarc/

- Create mechanisms for information sharing with other providers regarding fibre cuts, so as to make quick fixes and speed up maintenance
- Cooperate with law enforcement and regulatory agencies during the investigation and prosecution of cybercrime or other illegal activities

## 2 Institutional/Organizational Level

Executive leadership and accountability for cyber-related issues is required. An executive leader in every organization should be responsible for the information security of the organization. In that role, the executive leader can allocate resources for, and promote, an organizational cybersecurity culture. Security practices for organizations that utilize ICTs not only have a strong impact on the organizations themselves, but also on the wider Internet ecosystem. It is, therefore, important that these organizations are aware of the impact of their actions (or inaction) on the security of others. A clear and implemented security policy based on recurring risk assessment and underpinned by organizational commitment should contain, at the minimum, several specific action items. These include: applying basic essential measures for a healthy network; demonstrating an adequate system of controls; having a formalized process and capability to respond to cyber-incidents; conducting regular exercises; establishing a disclosure process; and ensuring established relationships with other stakeholders, such as government officials and CSIRT teams.

National governments, and other stakeholders, should empower organizations and institutions to create a culture of cybersecurity for economic and social prosperity through information sharing, promoting best practices, and leading by example. The necessary organizational structure should be put in place in institutions that are responsible for cybersecurity initiatives and activities.

Organizations and institutions should implement current best practices and develop a culture of cybersecurity at the operational, as well as the executive level.