Internet Infrastructure Initiative

Triple I: a GFCE Capacity-building project

@AIS2019, Kampala, 16 June 2019

Maarten Botterman

Global Risks Report 2018

"… this generation enjoys unprecedented technological, scientific, and financial resources, which we should use to chart a course towards a more sustainable, equitable and inclusive future.

At the same time, the risks are greater than ever, with an important role for disruptive technologies that may be used to affect societies in good and bad ways, and with cyberattacks amongst today's biggest threats to disrupt society."

Internet Infrastructure Initiative

- Aim: to help build a robust, transparent and resilient internet infrastructure.
- Rationale: A robust, open and resilient internet infrastructure is key to counter infringements and threats to the cyber domain, and:
  - diminishes the chances and impact of cyber-attacks (like DDoS) and cybercrime (hacking malware, phishing, botnets) and SPAM.
  - enables the public to maintain confidence and trust;
  - is a precondition for the use of the internet as a means to boosting innovative and economic activities.
- Offering: this Initiative seeks to deepen and broaden the know-how in locally applying, testing and monitoring compliance with widely agreed open internet standards.
  - Key elements include national internet infrastructure protection, internet exchange points, registries, open source software, email security and routing security.

Supported by global and regional stakeholders

- GFCE members
  - Governments
  - International Organisations
  - Businesses
- Regional Internet Registries
  - All regions
- Internet Society
  - Global office
  - Local chapters
- NL Ministry of Economic Affairs

Internet Society

lacnic

AFRINIC

APNIC

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

GFCE

AfricaCERT
United in promoting cyber security in Africa

Ministerie van Economische Zaken

Setting up Capacity building events

- Targeted at regions that are catching up
- Bringing together regional stakeholders
- Awareness raising on Open Internet Tools
- Inspiration through Good Practice Examples (mix local/global)
- Impact through joint commitment for action

From State-of-Practice to State-of-the-Art, together

Joint priority setting and action planning

Kampala, 16 June 2019


"What to do to improve justified trust in using the Internet and email in the region"
Purpose of the Day

GFCE Triple-I agenda for today

09:00 Opening, intent

09:30 Block I: Better Use of Today's Open Internet Standards

11:25 Block II: Inspiration from Good Practice Actions - 1

12:10 Lunch

13:15 Block II: Inspiration from Good Practice Actions - 2

16:00 Block III: Action Planning for a More Trusted Internet

17:00 Conclusions and Closing Remarks

Block I: Introduction to use and usefulness of Open Internet Standards

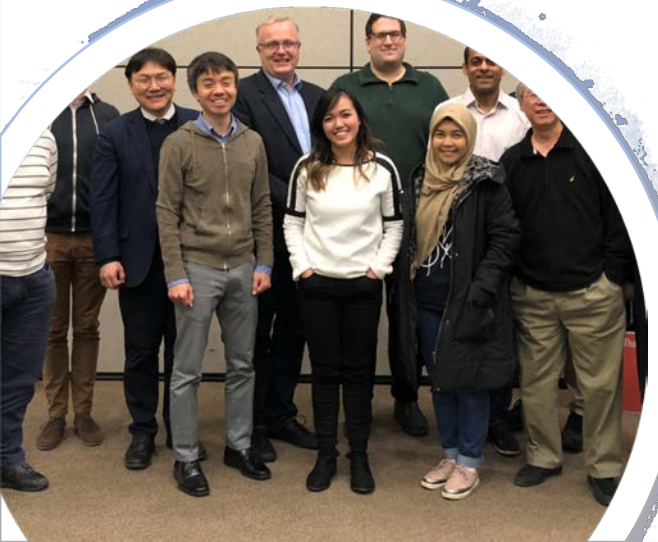
- Living room conversation with Alain Aina (WACREN) and Adiel Akplogan (ICANN) , involving all in the room
- DNSSEC/TLS/DANE; RPKI/ROA; DKIM/DMARCK/SPF; IPv6
- Interactive discussion of all standards as also covered by Internet.nl, grouped in terms of Internet routing, e-mail handling and other

Block II: Inspiration from Practice

- Collaborative action for DDOS Mitigation - Cristian Hesselman (SIDN)
- Resources to help detect and act against abuse - Jean-Robert Hountomey (AfricaCERT), Yuri Ito (Cybergreen) and Adiel Akplogan (ICANN)
- Mutually Agreed Norms for Routing Security (MANRS) - Michuki Mwangi (ISOC)
- Secure IoT deployment – Kevin Chege, Verengai Mabika (ISOC)

Block III: Market Place for regional action

- Every event adds with an inventory of possible actions
- Participants gather to discuss the <action proposals> they feel are relevant.
- Up to 3 subjects fleshed out for follow-up



4 events so far

- Dakar, Senegal, hosted by the African Internet Summit, supported by AfricaCERT/AfriNIC/ISOC 2019, 7 May 2018
- Almaty, Kazachstan, hosted by RIPE NCC, supported by RIPE NCC/ISOC/Kazachstan Telecom, 25 September 2018
- Delhi, India, hosted by Indian Summerschool for Internet Governance, supported by ISOC/APNIC/Indian Govt, 12 October 2018
- Daejeon, Korea, hosted by APRICOT2019,supported by APNIC/ISOC/dotASIA, 23 February 2019

Help make the Internet more reliable in your region

1

Contribute with good practice examples to events

2

Support an event in your region as co-organizer or participant

3

Improve the reliability of Internet by taking action

Next events under preparation

- Kolkata, India, hosted by Indian Summerschool for Internet Governance, supported by INSIG, ISOC, APNIC, Indian Gov, 14 November 2018
- 2 more events under exploration

Triple I is a GFCE project

www.thegfce.com

For more information contact:

Maarten Botterman: maarten@gnksconsult.com
Arnold van Rhijn: A.C.F.vanRhijn@minez.nl

About Maarten Botterman

- More than 25 years experience with work “in the public interest”: where connected technologies touch society - internationally
- Independent analyst, strategic advisor, moderator and chairman, see for more: www.gnksconsult.com
- Currently chairing: IGF Dynamic Coalition on Internet of Things (www.iot-dynamic-coalition.org/); PICASSO Policy Expert Group (www.Picasso-project.eu), and Supervisory Board of NLnet Foundation (www.nlnet.nl.)
- ICANN Board Member (www.icann.org)
- Full CV: https://www.linkedin.com/in/botterman
- Email: maarten@gnksconsult.com

CyberGreen

A global community to measure and improve cyberhealth

Improving Cyber Ecosystem Health through Metrics, Measurement and Mitigation Support

Africa Internet Summit
June 2019

Yurie Ito

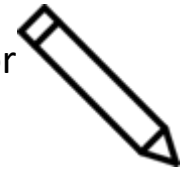
Executive Director, CyberGreen

The CyberGreen Institute is a global non-profit organization focused on helping to improve the health of the global Cyber Ecosystem.

Cyber Health Measurement.
We measure **Risk-to-others.**

Conduct weekly Internet scans for risk condition data

Provide a clearinghouse for Risk Mitigation BCPs.



Capacity Building needs analysis and impact measurement

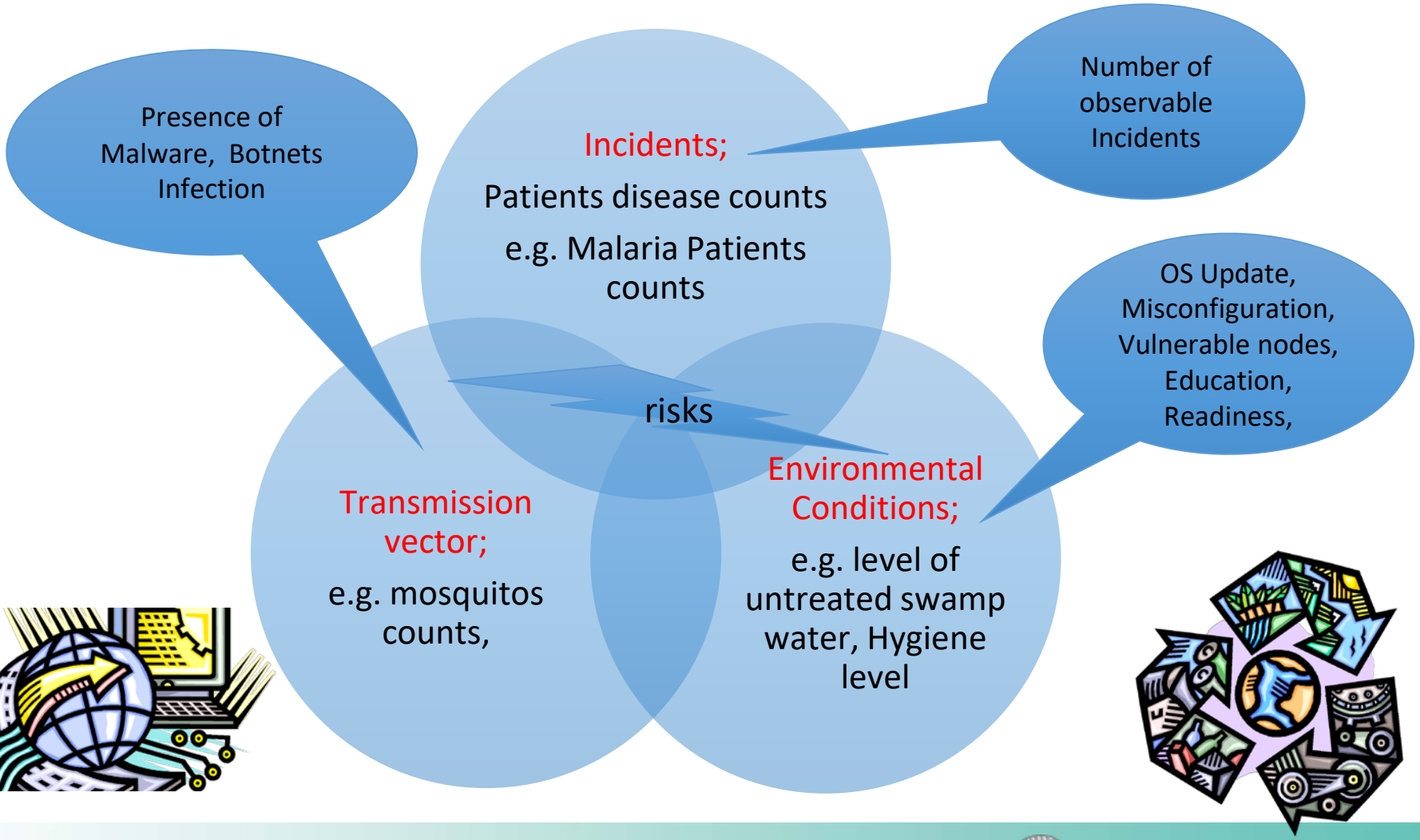
Advocacy

CyberGreen

Key Questions

- How do you communicate effectively and support decision makers?
- What do you need to motivate non-technical policy makers to understand and sign off the action?

Applying Public Healthcare approach to Cyber



CyberGreen

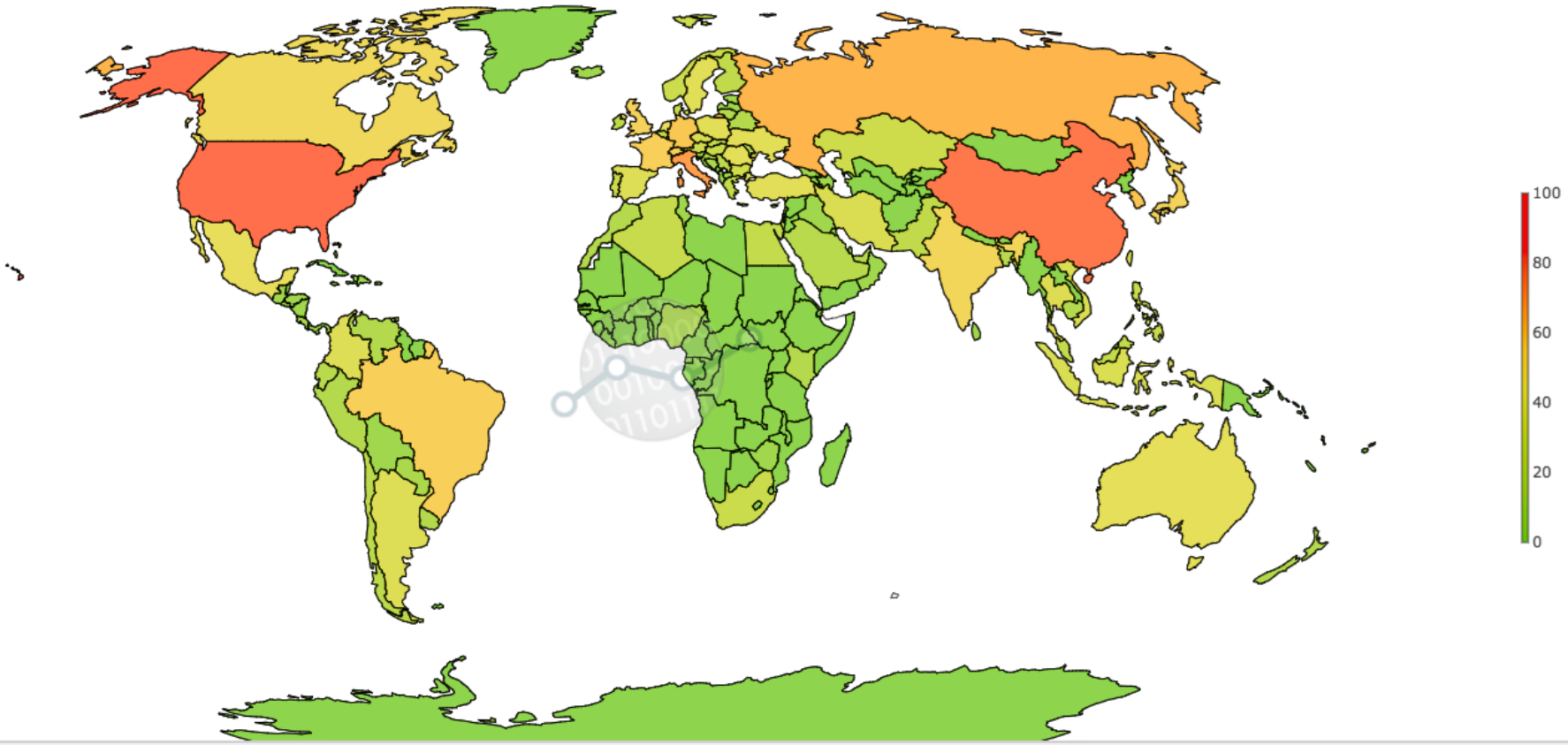
CyberGreen: What we do

- Perform Internet scans
- Collect and analyze data for five open recursive protocols (NTP, DNS, SSDP, SNMP, CHARGEN) commonly used to execute DDoS reflection attacks.
- These open servers have the potential to be used as infrastructure to launch DDoS attacks within a country's borders and abroad.
- Inform network operators, policymakers, other stakeholders on the risks associated with hosting open servers.

CyberGreen: What we measure

Type	Description
Open DNS	Domain Name System (DNS) is a standard protocol that translates human-friendly host names like www.cybergreen.net into numerical, Internet Protocol (IP) addresses such as 197.222.126.114 DNS can have an amplification factor of up to 179. In other words: 1 Byte turns into 179 Bytes in DDOS traffic.
Open NTP	Network Time Protocol (NTP) is standard protocol for time synchronization for devices on a network, used by servers, mobile devices, endpoints and networking devices from all vendors. NTP has an amplification factor of 556.9.
Open SNMP	Simple Network Management Protocol is for collecting and organizing information about devices on networks, including cable modems, routers, switchers, servers, printers etc. SNMP has an amplification factor of 6.3.
Open SSDP	Simple Service Discovery Protocol (SSDP) is the standard search protocol for Universal Plug and Play (UPnP) UPnP is pervasive - it is enabled by default on home gateways, network printers, webcams, network storage servers, and “smart home” devices such as thermostats, automated assistants and wireless home security systems that are part of the Internet of Things (IoT). SSDP's amplification factor is ~ 30.
Open CHARGEN	Character Generator Protocol (CHARGEN) is a service of the Internet Protocol Suite defined in RFC 864 in 1983 by Jon Postel. It is intended for testing, debugging, and measurement purposes. The protocol is rarely used, as its design flaws allow ready misuse. CHARGEN's amplification factor is ~360, making it one of the more effectively abuseable protocols for UDP amplification.

Global View
http://stats.cybergreen.net



CyberGreen

Raw count of open resolvers: Uganda May 14, 2019

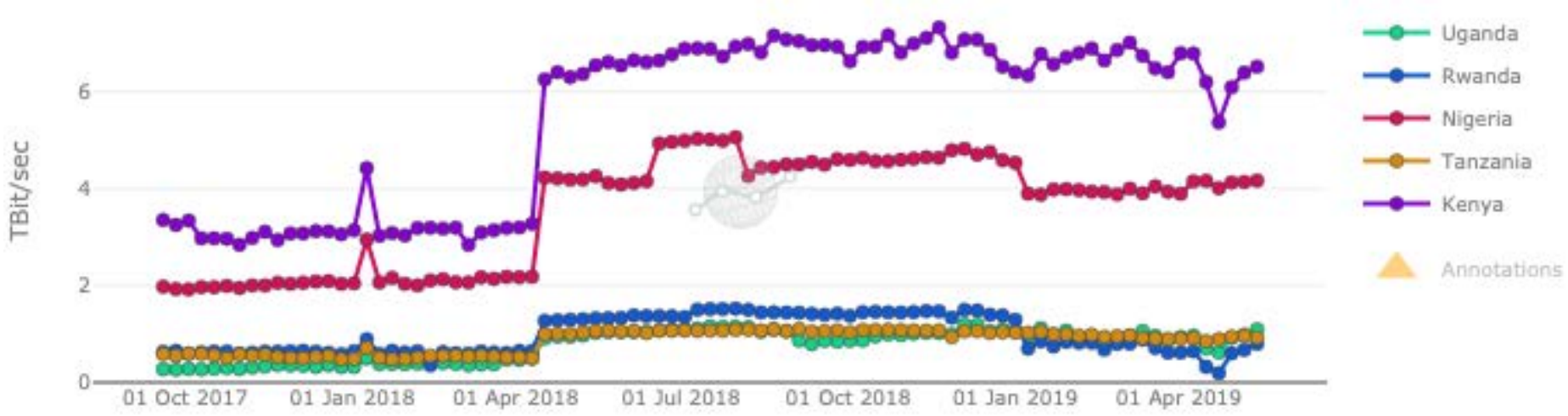
DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (TBit/Sec)	DDoS Rank
1,081	1,874	651	4	N/A	1	116

- Uganda ranks #116 out of 239 for riskiest DDoS environments.
- Based on the presence of five types of open recursive servers (NTP, DNS, SSDP, SNMP, CHARGEN) in Uganda.
- Most prevalent open protocol in Uganda's network is NTP (1,874).

CyberGreen

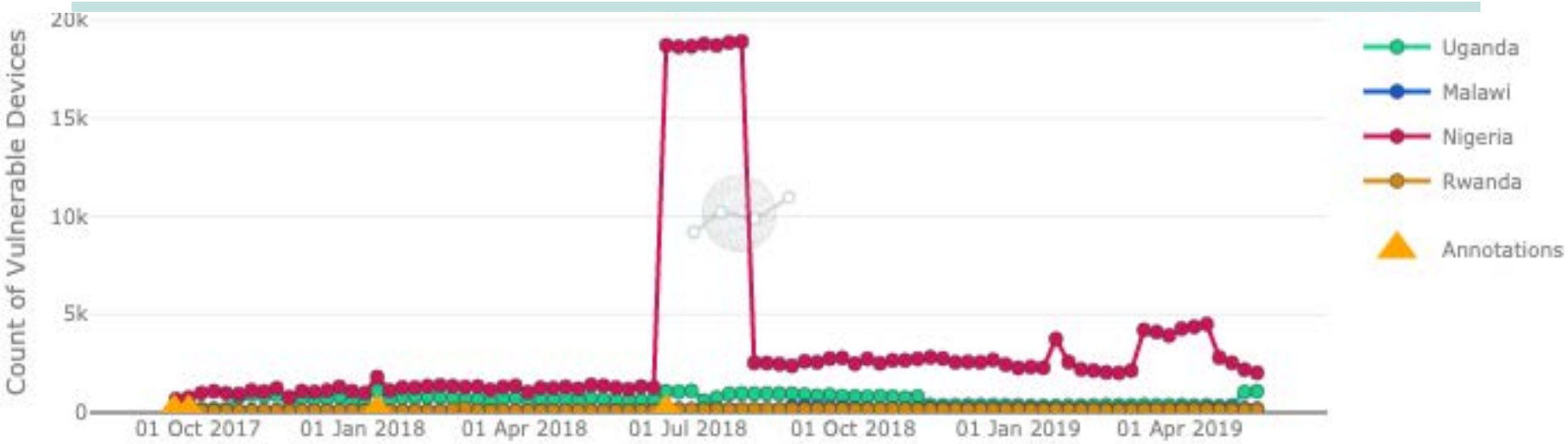
Compare with Rwanda, Nigeria, Tanzania, Kenya

Total Potential DDoS Bandwidth



CyberGreen

Comparison: Uganda, Malawi, Nigeria, Rwanda
Open DNS



Raw counts as of May 14, 2019:

	DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (TBit/Sec)	DDoS Rank
Uganda	1,081	1,874	651	4	N/A	1	116
Malawi	179	130	229	N/A	N/A	0	198
Nigeria	2,026	7,279	4,170	31	N/A	4	77
Rwanda	122	1,423	50	N/A	N/A	1	128

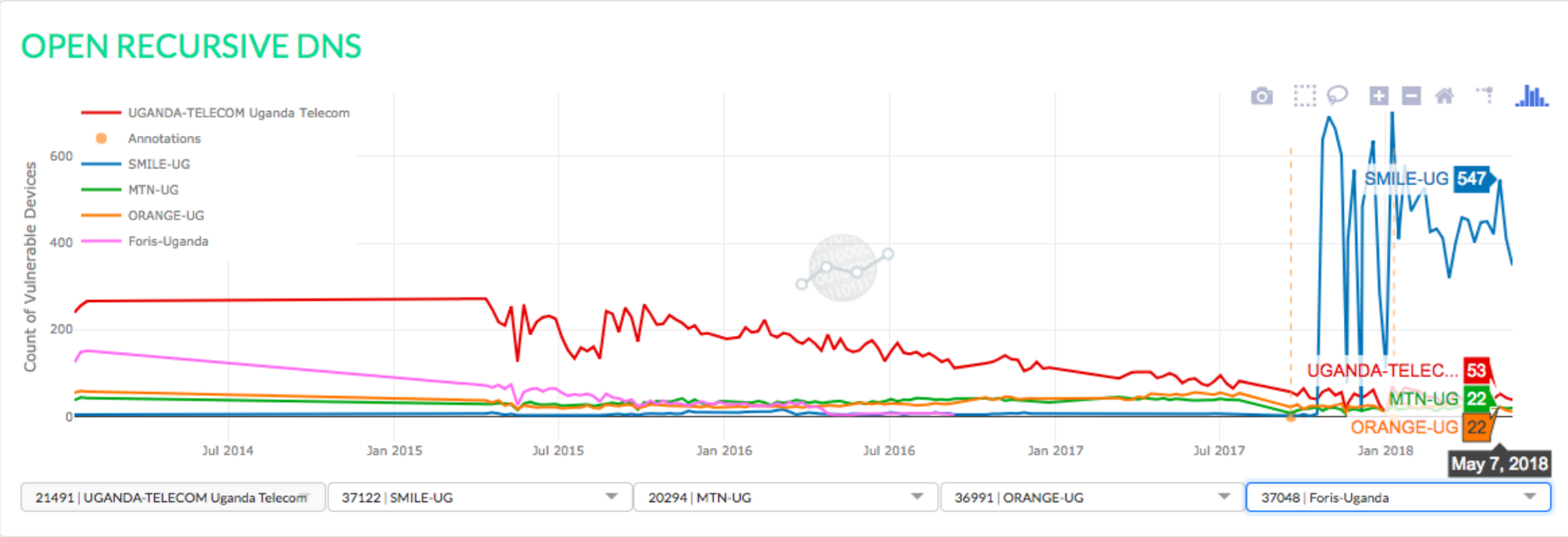
CyberGreen

ASNs/ISPs in Uganda

So let's look at Uganda's ISPs

- An Autonomous System Number (ASN) is a number used by network operators to uniquely identify an independent IP network that has its own routing policies
- Uganda has 46 ASNs
- And not all are equal…

Comparison across 4 Ugandan ASNs
Open DNS



CyberGreen

What can be done?
- conduct national level mitigation campaign

Download CyberGreen Mitigation Materials at

http://www.cybergreen.net/mitigation/

Mitigation approaches:

- How to identify your vulnerable servers/devices across your network
- How to find hosts running under risk conditions
- Step-by-step actions (e.g. update devices, reconfiguration, block certain protocols, disable services, implement certain BCPs)
- How to verify your fix

CyberGreen

Annual Health Check-up

(Human health Model)
Individual health – preventative measures

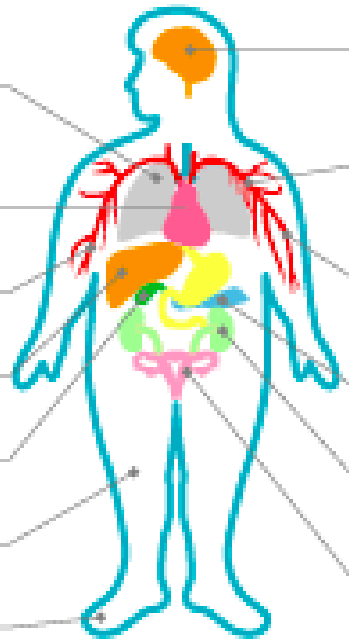
Medical checkup : Risk indicators and health metrics

Physical measurement	blood pressure	White blood cells, red blood
Liver function, hepatitis test,	Inflammatory response etc	Thyroid (hormone)
Lipid metabolism	Glucose metabolism	Renal function
Tumor marker	Other inspection	Gynecology, optional
Mammary gland disease		

Epidemiological studies

Risk Mitigation of HL
- Eat good cholesterol
- Eat high fiber
- Exercise
- Stop smoking
- etc...

Diseases caused by Obesity

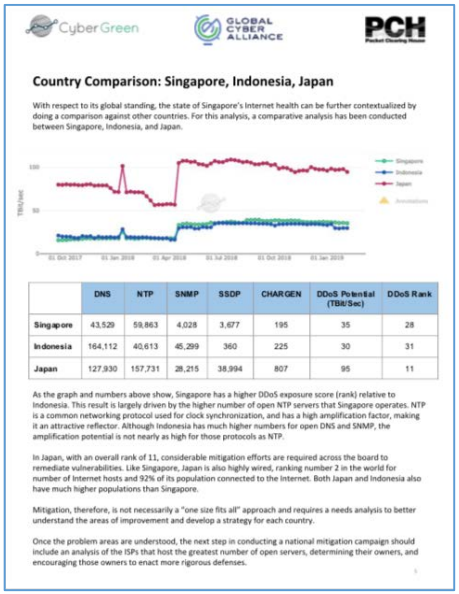


- Breathing Problem (sleep apnea Syndrome)
- Cardiac Disease （Angina, Cardiac Infarct）
- High Blood Pressure
- Fatty Liver
- Cholelithiasis
- Arthritis Disorder
- High uric acid blood（Gout）
- Cerebrovascular disease
- arteriosclerosis
- Hyperlipidemia
- Diabetes
- Kidney disease
- Menstruation disorder

Cyber ecosystem health annual check-up

CyberGreen and our partners expert team would visit target country Cybersecurity stakeholders and conduct Systemic risk analysis, put together the mitigation plan and policy recommendation to your country's specific needs.

Vulnerability Landscape:
Open resolver analysis



Country Comparison: Singapore, Indonesia, Japan

With respect to its global standing, the state of Singapore's Internet health can be further contextualized by doing a comparison against other countries. For this analysis, a comparative analysis has been conducted between Singapore, Indonesia, and Japan.

	DNS	NTP	SNMP	SSDP	CHARGEN	DDoS Potential (TBit/Sec)	DDoS Rank
Singapore	43,529	59,863	4,028	3,677	195	35	28
Indonesia	164,112	40,613	45,299	360	225	30	31
Japan	127,930	157,731	28,215	38,994	807	95	11

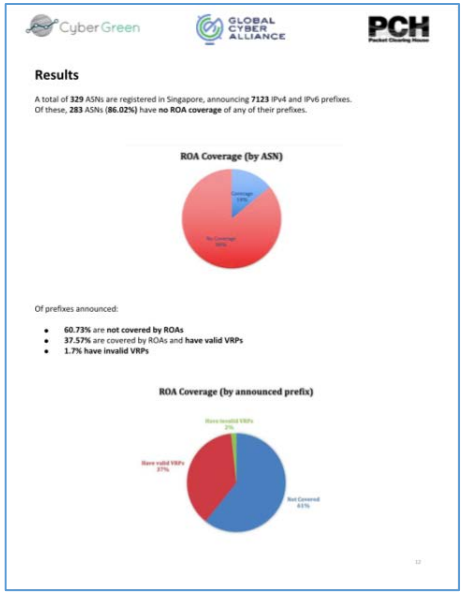
As the graph and numbers above show, Singapore has a higher DDoS exposure score (rank) relative to Indonesia. This result is largely driven by the higher number of open NTP servers that Singapore operates. NTP is a common networking protocol used for clock synchronization, and has a high amplification factor, making it an attractive reflector. Although Indonesia has much higher numbers for open DNS and SNMP, the amplification potential is not nearly as high for those protocols as NTP.

In Japan, with an overall rank of 11, considerable mitigation efforts are required across the board to remediate vulnerabilities. Like Singapore, Japan is also highly wired, ranking number 2 in the world for number of Internet hosts and 92% of its population connected to the Internet. Both Japan and Indonesia also have much higher populations than Singapore.

Mitigation, therefore, is not necessarily a "one size fits all" approach and requires a needs analysis to better understand the areas of improvement and develop a strategy for each country.

Once the problem areas are understood, the next step in conducting a national mitigation campaign should include an analysis of the ISPs that host the greatest number of open servers, determining their owners, and encouraging those owners to enact more rigorous defenses.

Internet Infrastructure:
BGP ROA analysis



Results

A total of **329** ASNs are registered in Singapore, announcing **7123** IPv4 and IPv6 prefixes. Of these, **283** ASNs (**86.02%**) have **no ROA coverage** of any of their prefixes.

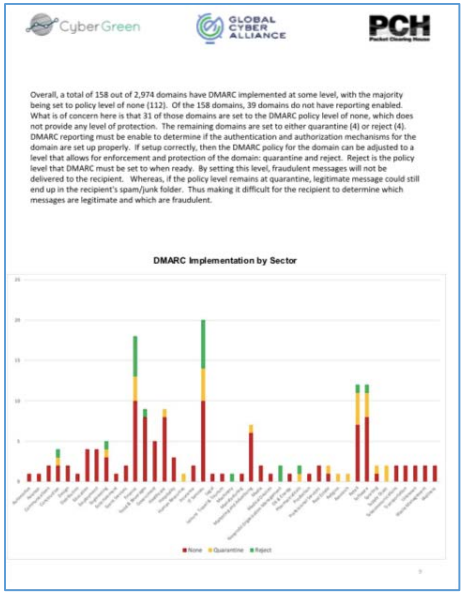
ROA Coverage (by ASN)

Of prefixes announced:

- **60.73%** are **not covered by ROAs**
- **37.57%** are covered by ROAs and **have valid VRPs**
- **1.7% have invalid VRPs**

ROA Coverage (by announced prefix)

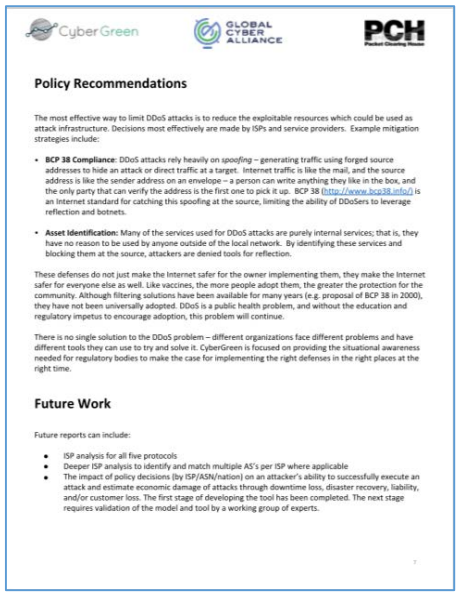
Email infrastructure:
DMARC analysis



Overall, a total of 158 out of 2,974 domains have DMARC implemented at some level, with the majority being set to policy level of none (112). Of the 158 domains, 39 domains do not have reporting enabled. What is of concern here is that 31 of those domains are set to the DMARC policy level of none, which does not provide any level of protection. The remaining domains are set to either quarantine (4) or reject (4). DMARC reporting must be enable to determine if the authentication and authorization mechanisms for the domain are set up properly. If setup correctly, then the DMARC policy for the domain can be adjusted to a level that allows for enforcement and protection of the domain: quarantine and reject. Reject is the policy level that DMARC must be set to when ready. By setting this level, fraudulent messages will not be delivered to the recipient. Whereas, if the policy level remains at quarantine, legitimate message could still end up in the recipient's spam/junk folder. Thus making it difficult for the recipient to determine which messages are legitimate and which are fraudulent.

DMARC Implementation by Sector

Policy Recommendation



Policy Recommendations

The most effective way to limit DDoS attacks is to reduce the exploitable resources which could be used as attack infrastructure. Decisions most effectively are made by ISPs and service providers. Example mitigation strategies include:

- **BCP 38 Compliance**: DDoS attacks rely heavily on *spoofing* – generating traffic using forged source addresses to hide an attack or direct traffic at a target. Internet traffic is like the mail, and the source address is like the sender address on an envelope – a person can write anything they like in the box, and the only party that can verify the address is the first one to pick it up. BCP 38 (http://www.bcp38.info/) is an Internet standard for catching this spoofing at the source, limiting the ability of DDoSers to leverage reflection and botnets.
- **Asset Identification:** Many of the services used for DDoS attacks are purely internal services; that is, they have no reason to be used by anyone outside of the local network. By identifying these services and blocking them at the source, attackers are denied tools for reflection.

These defenses do not just make the Internet safer for the owner implementing them, they make the Internet safer for everyone else as well. Like vaccines, the more people adopt them, the greater the protection for the community. Although filtering solutions have been available for many years (e.g. proposal of BCP 38 in 2000), they have not been universally adopted. DDoS is a public health problem, and without the education and regulatory impetus to encourage adoption, this problem will continue.

There is no single solution to the DDoS problem – different organizations face different problems and have different tools they can use to try and solve it. CyberGreen is focused on providing the situational awareness needed for regulatory bodies to make the case for implementing the right defenses in the right places at the right time.

Future Work

Future reports can include:

- ISP analysis for all five protocols
- Deeper ISP analysis to identify and match multiple AS's per ISP where applicable
- The impact of policy decisions (by ISP/ASN/nation) on an attacker's ability to successfully execute an attack and estimate economic damage of attacks through downtime loss, disaster recovery, liability, and/or customer loss. The first stage of developing the tool has been completed. The next stage requires validation of the model and tool by a working group of experts.

CyberGreen

CyberGreen

Thank you!

Yurie Ito

yito@cybergreen.net

http://cybergreen.net

Http://stats.cybergreen.net