CyberGreen

A global community to measure and improve cyberhealth

Improving Cyber Ecosystem Health through Metrics, Measurement and Mitigation Support

GFCE workshop, Senegal

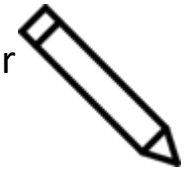
May, 7, 2018

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

We work with partners, including governments, seeking to address Cyber Risks.

Sponsors

JPCERT CC®

Foreign & Commonwealth Office

CSA SINGAPORE

Collaborators

AfricaCERT

APNIC

FARSIGHT SECURITY

GLOBAL CYBER ALLIANCE

GFCE

RCC

المركز العربي الإقليمي للأمن السيبراني
ITU - ARAB REGIONAL CYBERSECURITY CENTER

APWG

ICANN

APCERT
Asia Pacific Computer Emergency Response Team

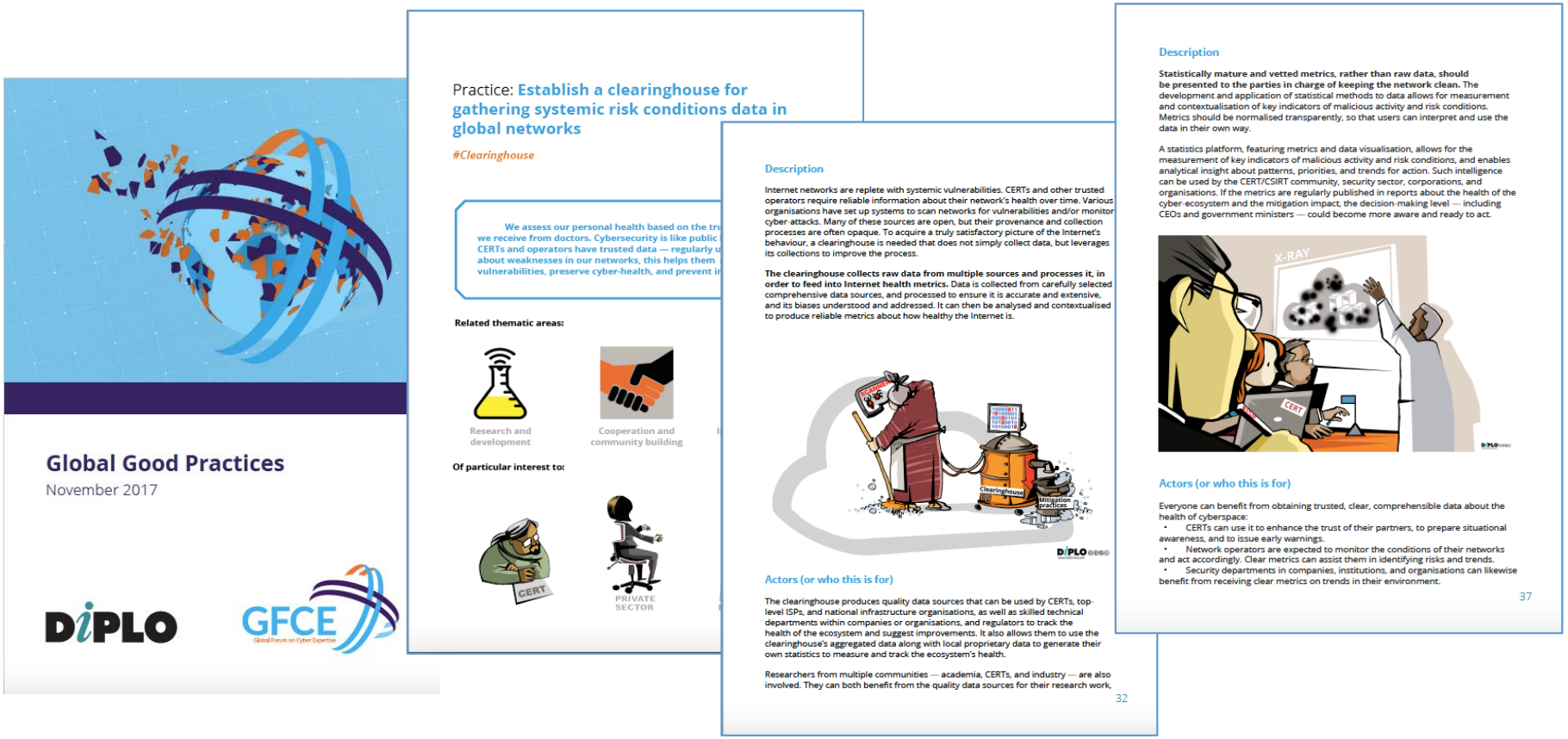
Internet Society

OIC-CERT
Computer Emergency Response Team

CyberGreen

Recognized as Global Good Practice

presented at GFCE / GCCS conference in New Delhi
https://www.thegfce.com/good-practices/incident-capture-and-analytics



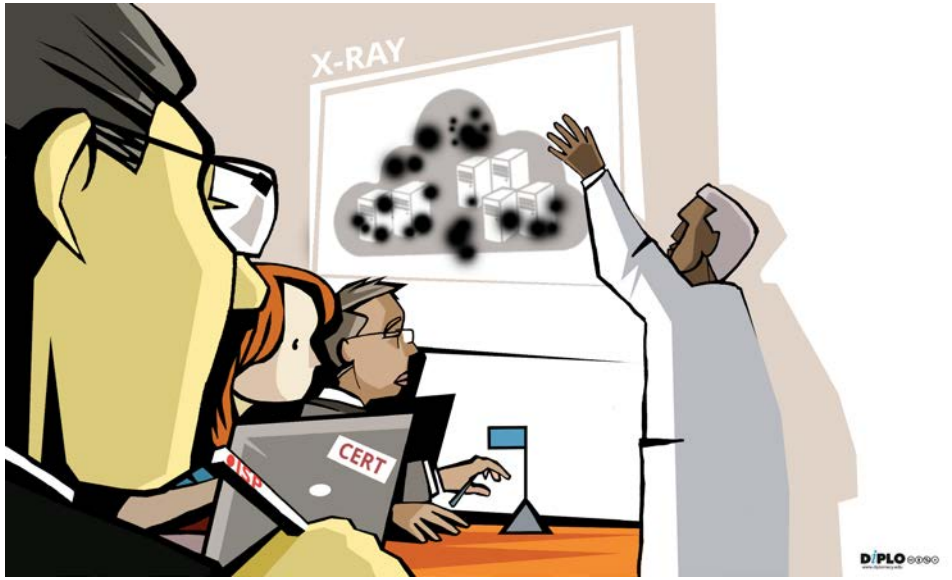
p.31-35: Establish a clearing house for gathering systemic risk conditions data in global networks
p.36-40: Produce and present trusted metrics about systemic risk conditions
p.41-44: Assist with cyber-risk mitigation and keep score of successes

CyberGreen

Key Questions

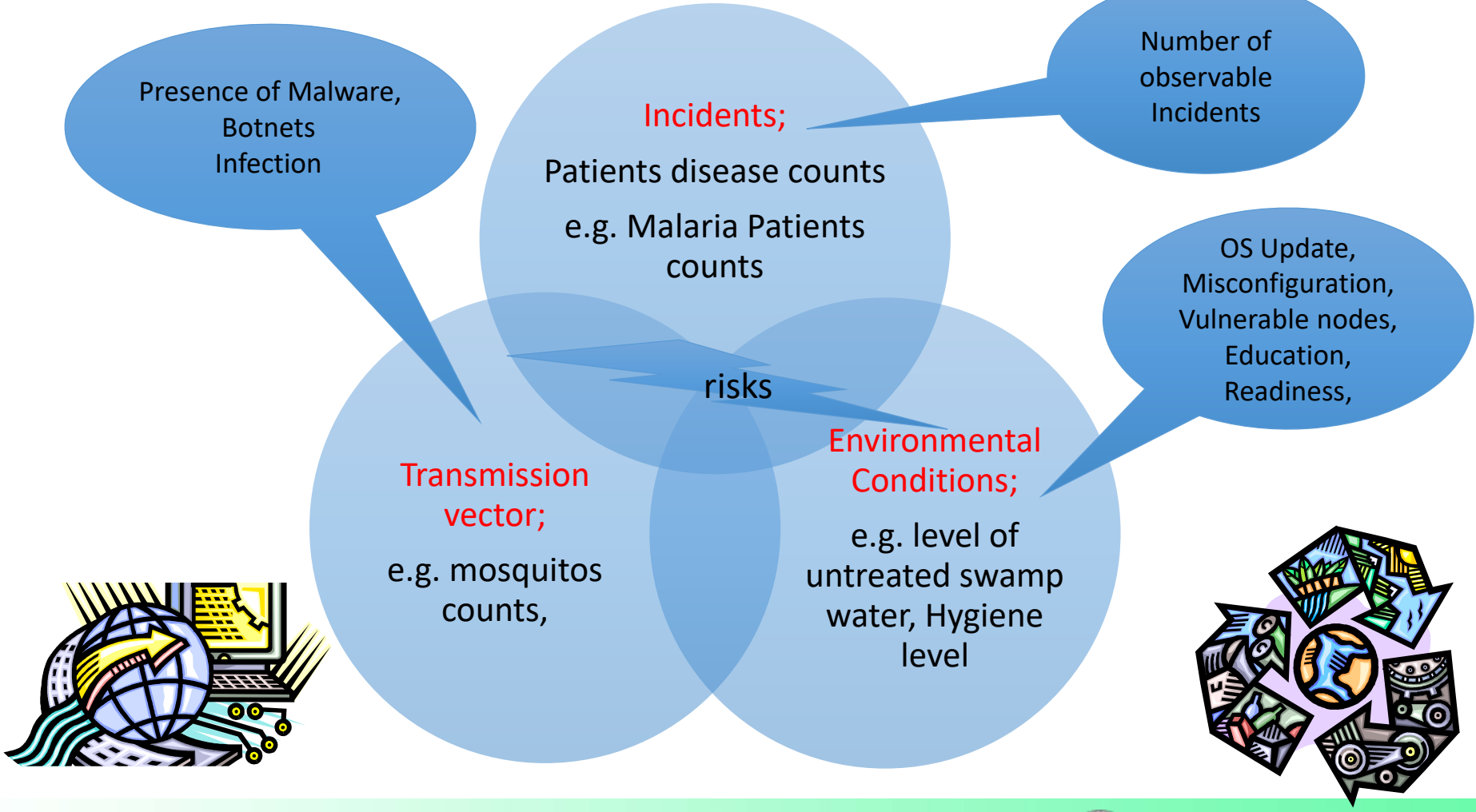
- Do you know the state of your cyber ecosystem health of your country?

- Do you know how to improve it? And it's impact?



CyberGreen

Applying Public Healthcare approach into Cyber



Lack of understanding of State of health, risks and measurement for Cyber Ecosystem

Public healthcare analogy

Figure 3.1
nternational public health security: a global network of national health systems a
echnical partners, focused on four major areas of work, coordinated by WHO

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.

CyberGreen

What are open recursive resolvers?

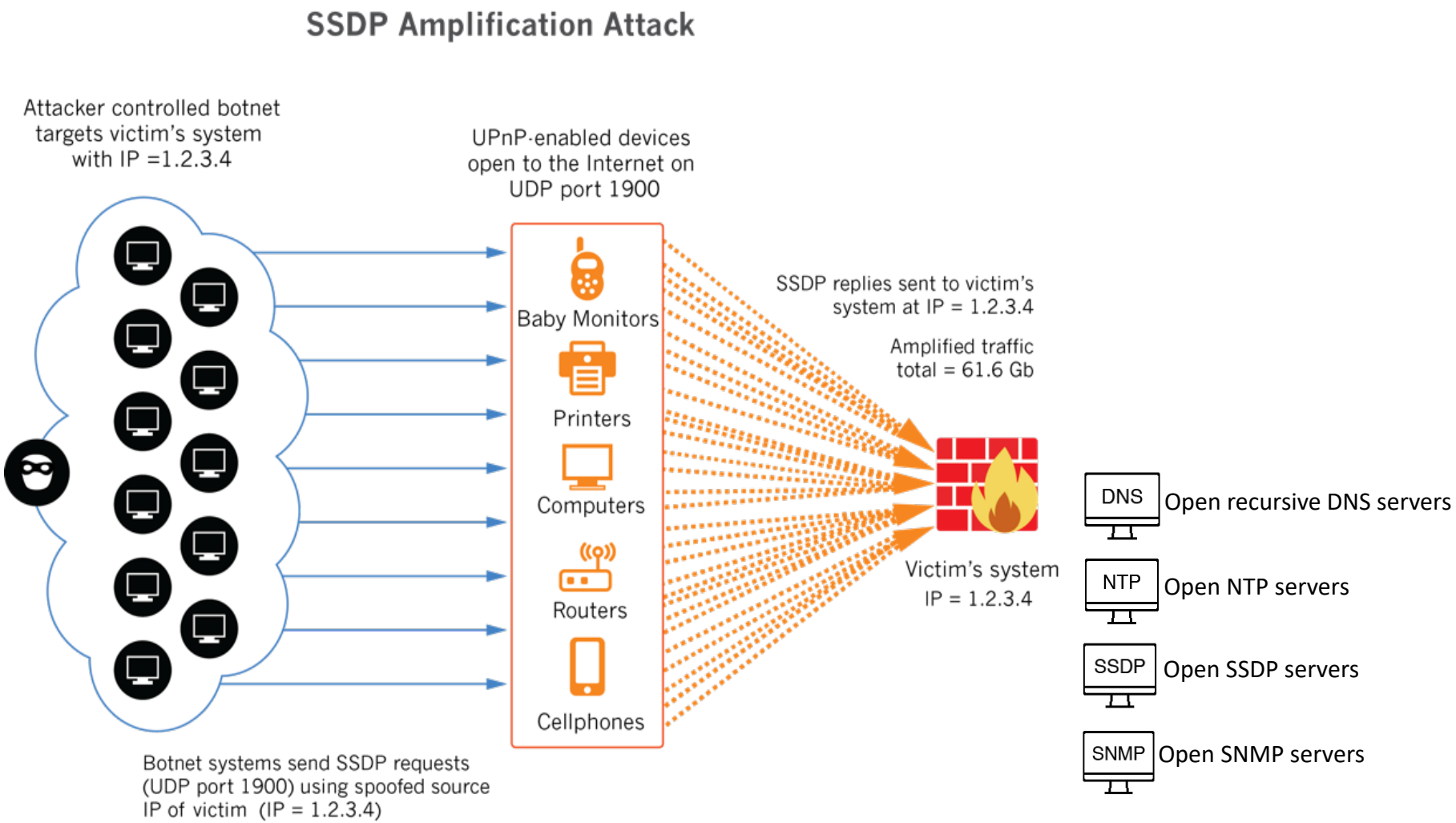
"Open recursive resolvers" are recursive resolvers (DNS servers) that will send a reply to any IP address

- Even about domains for which that DNS server is **not** an authoritative DNS server

Recursion is often on by default when DNS servers are first set up

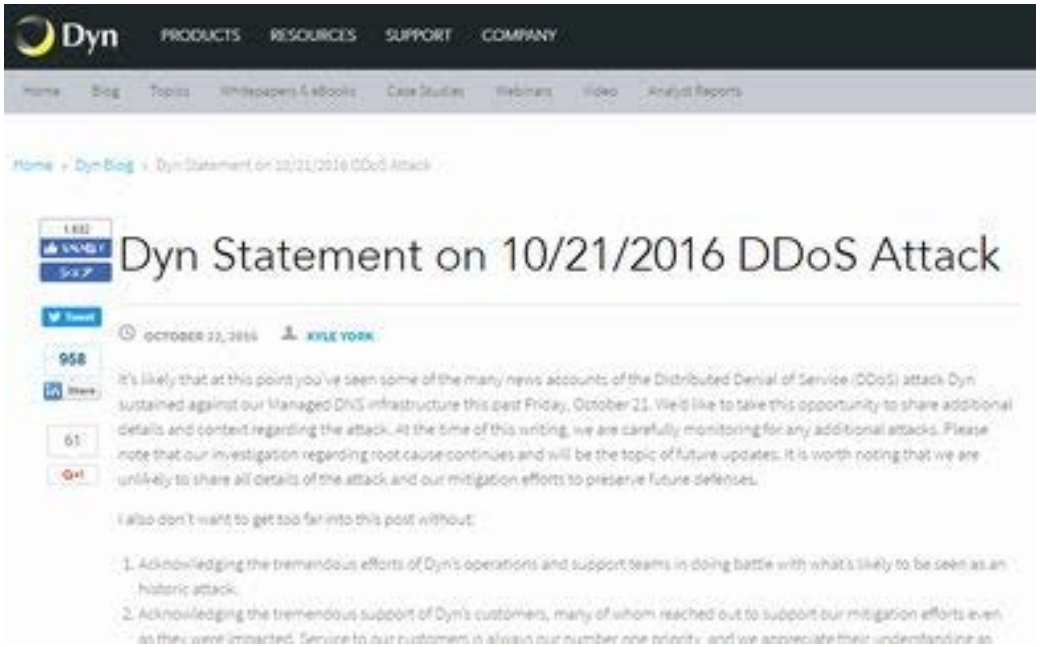
CyberGreen

Abuse-able systemic conditions posing risks to others *including to yourself*



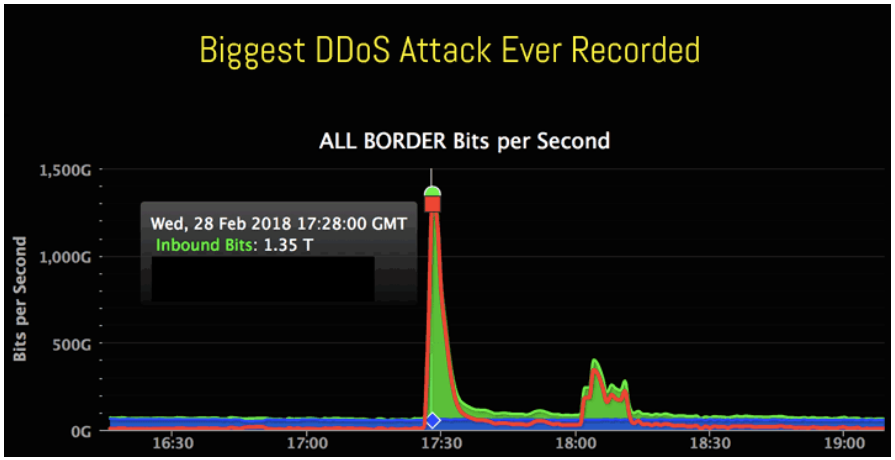
DDoS attack against DynDNS October 21, 2016

- Mirai Bot infected IoT devices
- Twitter, Spotify, Reddit, netflix, Wall Street Journal, Github… and other major services down



CyberGreen

DDoS case study : Memecached servers, February, 2018



- The largest recorded attack – peak of 1.35 Tbps
- Weaponized misconfigured memecached servers
- Targeted GitHub
- More than 2x larger than Mirai
- We should expect more massive attacks like this – and we should be prepared

Why do you have to CARE?

Economic Productivity

- Service interruption or failure of business operations relying on network connectivity, particularly for seasonal operations
- Time sensitive operations

Brand

- Loss of reputation with customers and partners

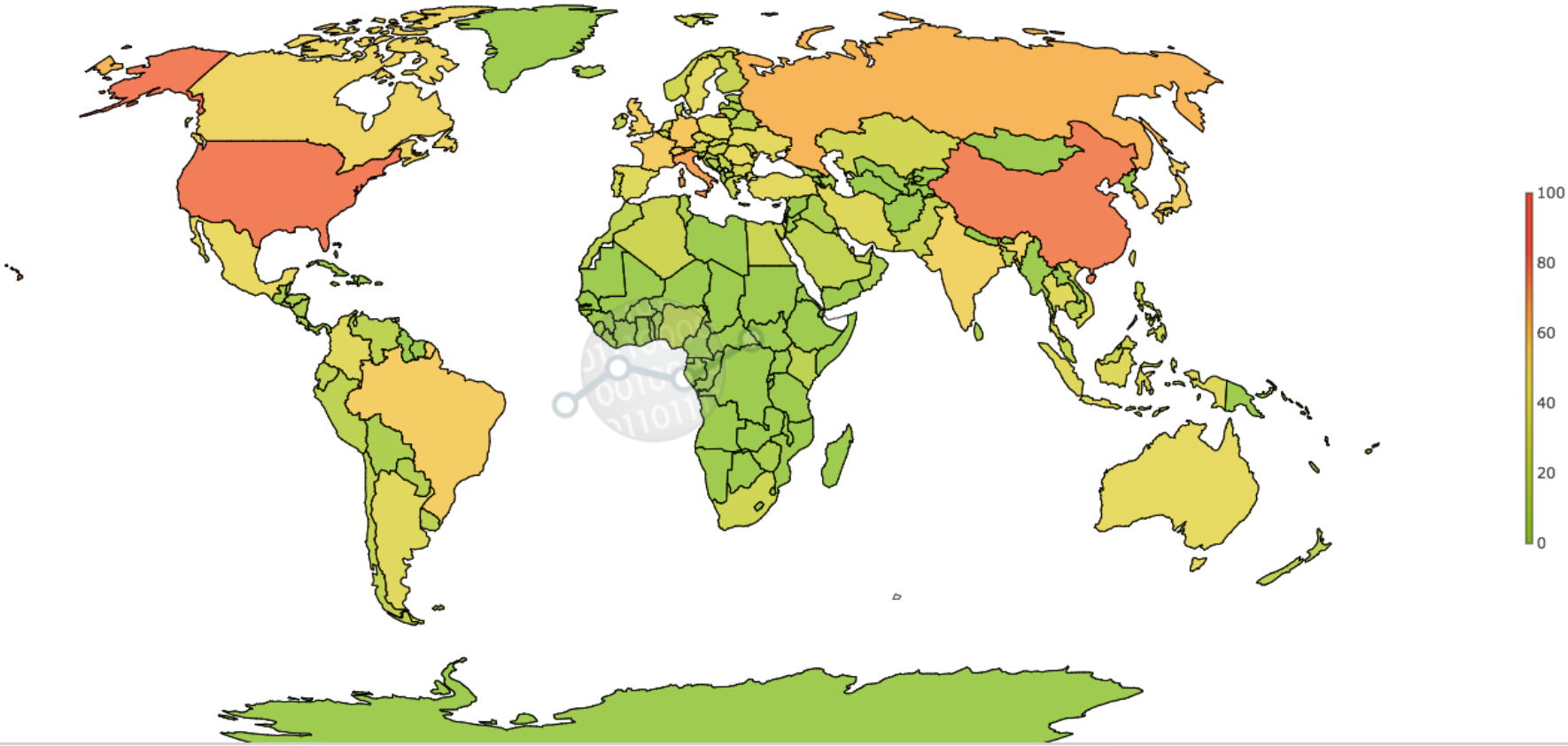
Technical

- Network service interrupted
- Isolation of victim network by network providers from the rest of Internet to mitigate collateral damage to other customers

Financial

- Loss of business resulting from service interruption
- Cost of specialized DDoS mitigation services

Global View
http://stats.cybergreen.net



CyberGreen

Senegal Overview

Week of April 23, 2018 – April 29, 2018

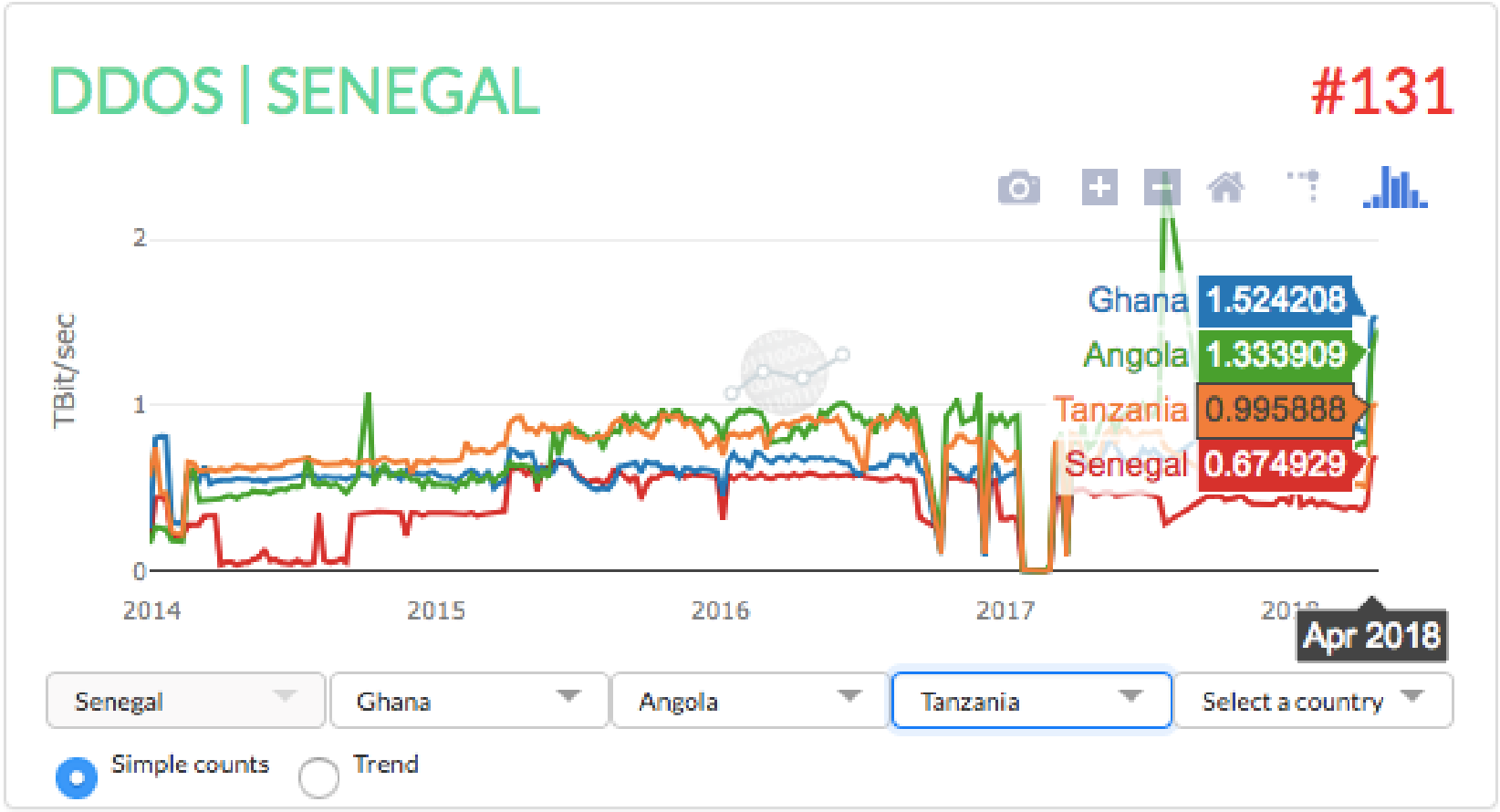
Country	Open Recursive DNS	Open NTP	Open SNMP	Open SSDP	Open CHARGEN	DDOS Potential TBit/sec
Senegal	1,144	1,136	136	278	N/A	1

- Open DNS is the biggest problem area, followed by open NTP

Let's compare Senegal to other African countries…

Compare with Senegal, Angola, Tanzania, Ghana

Total Potential DDoS Bandwidth



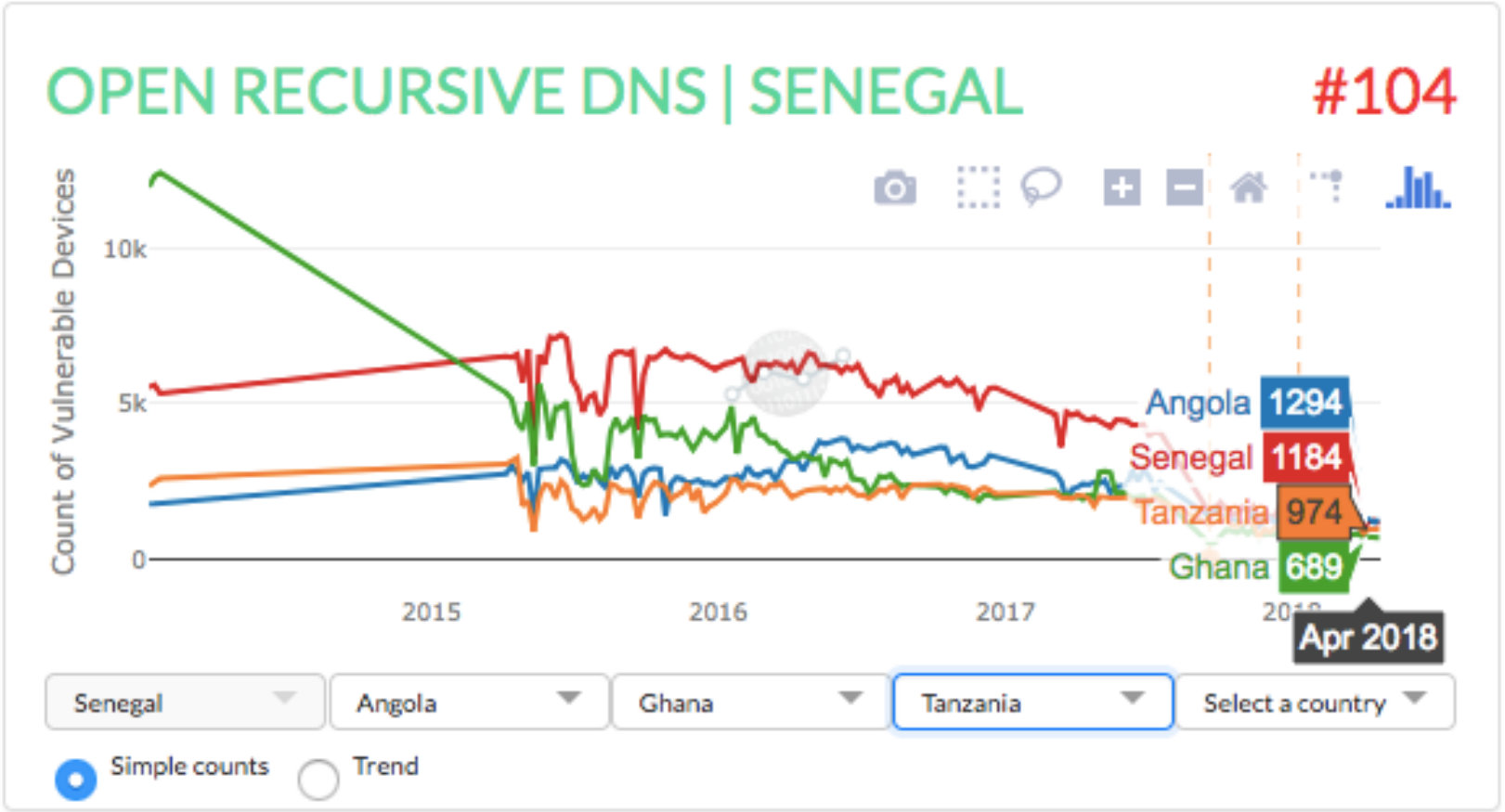
CyberGreen

A note on methodology

CyberGreen's v2.1 metrics report risk to others in terms of "How bad could it be?" This means that CyberGreen v2.1 metrics factor in the scale potential for amplification by protocol by node. Whereas the v2.0 Index is a rank order by the size of the unmet mitigation need, the v2.1 Index is a rank order by the size of the DDoS that could be mounted from the country, the AS, or the alternate entity should all of their nodes currently available to attackers were to be used in a single attack. In short, the v2.1 Index measures "offensive potential" — with the obvious caveat that we do not mean intentional offense but rather the degree to which the country, the AS, or the alternate entity can be made to engage in offense whether it wanted to or not.

Note: This formula for offensive potential does not take into account maximum upstream speeds of the observed unit. Our metrics experts at CyberGreen are currently discussing development of metric Version 2.1.5 to address this.

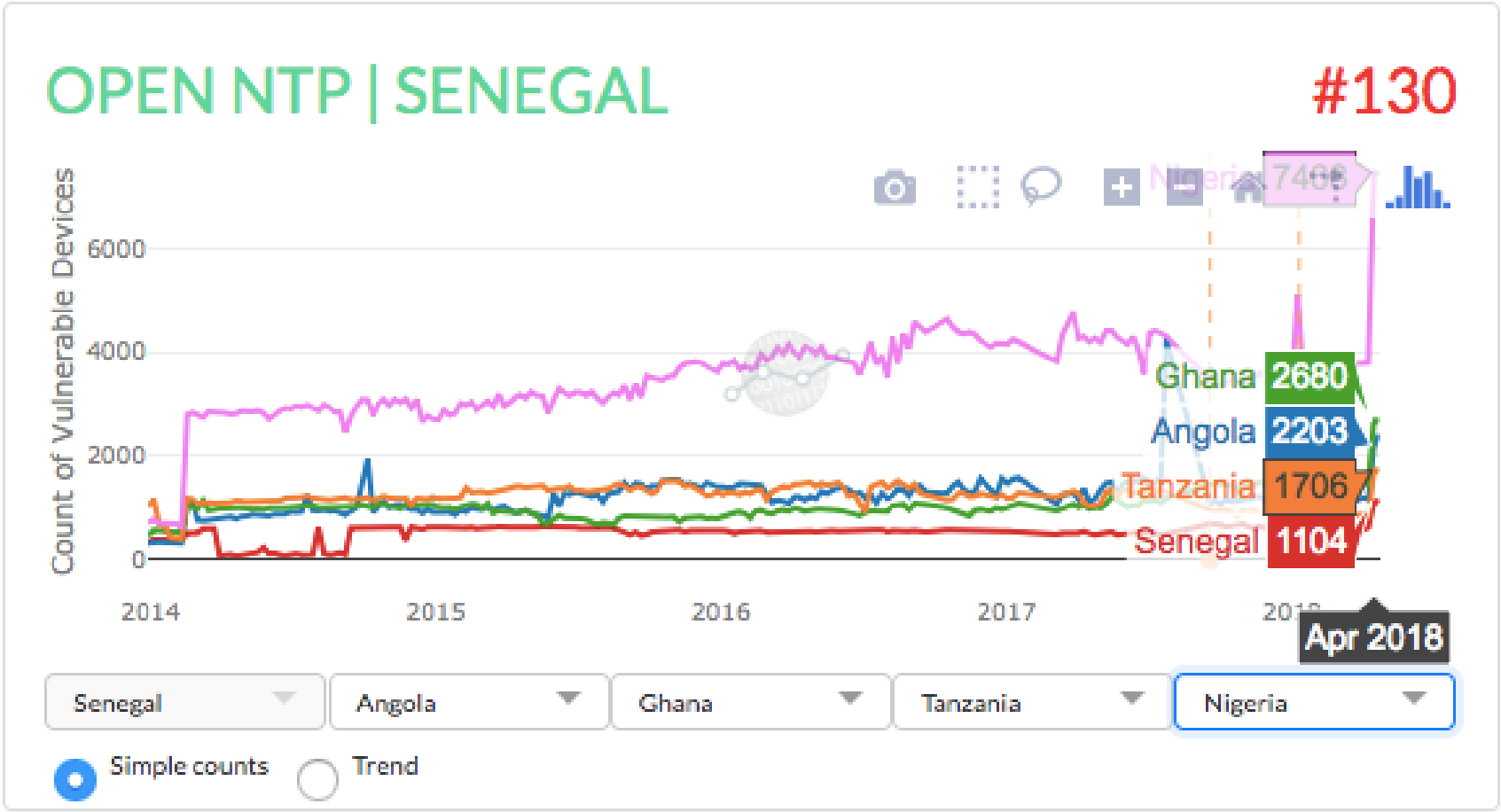
Compare with Senegal, Angola, Tanzania, Ghana
Open DNS



CyberGreen

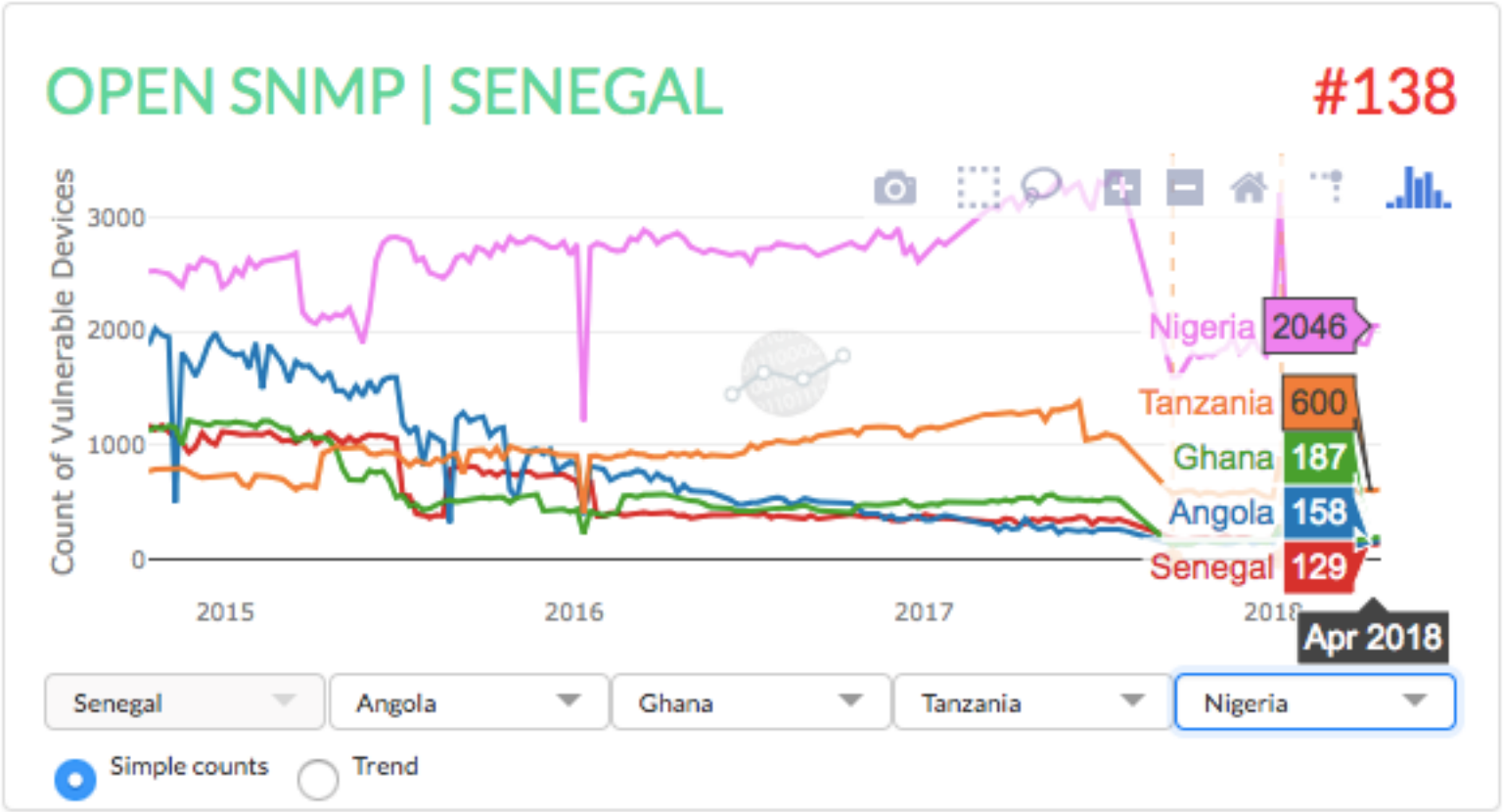
Compare with Senegal, Angola, Tanzania, Ghana, Nigeria

Open NTP



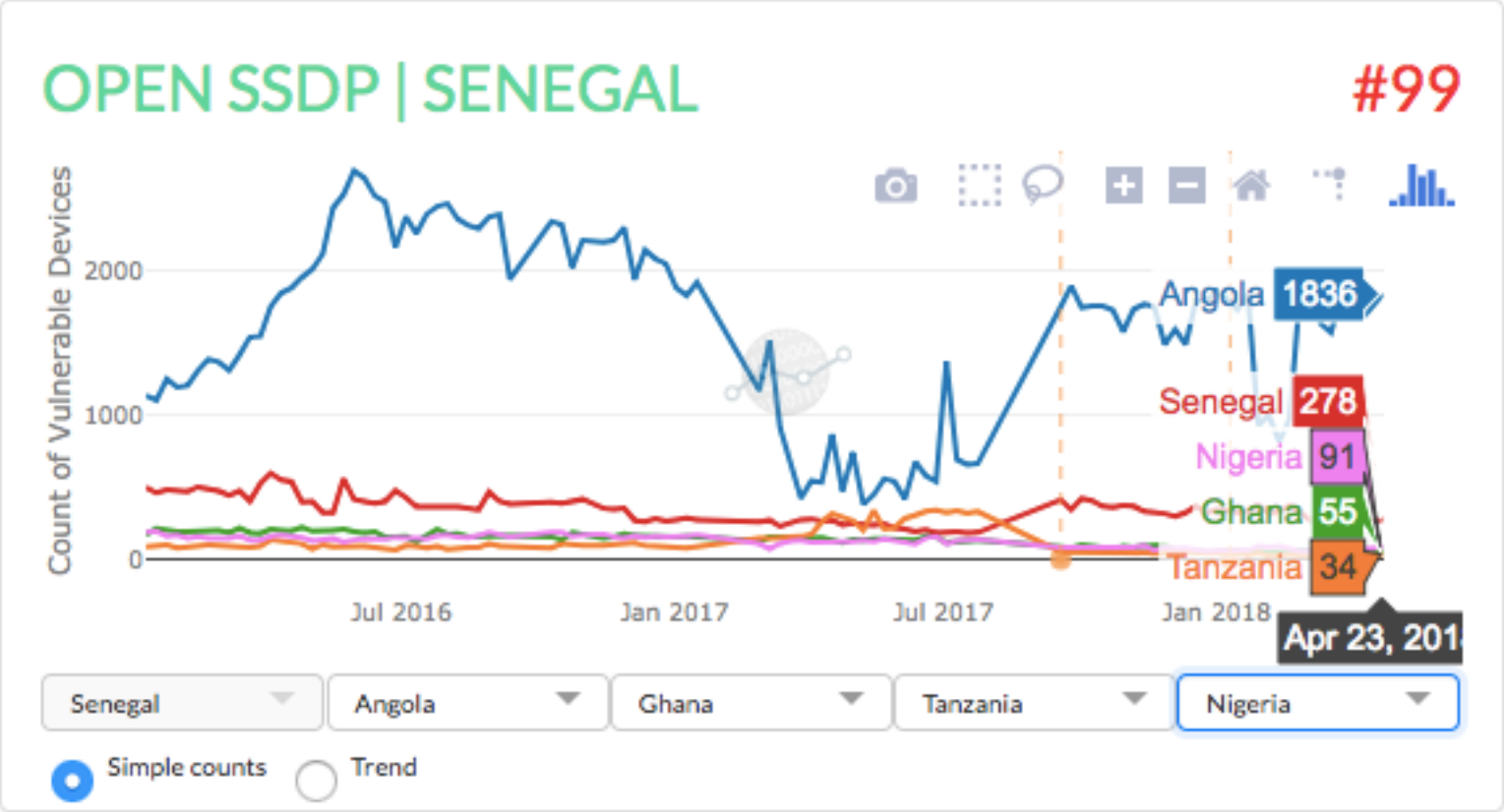
Compare with Senegal, Angola, Tanzania, Ghana, Nigeria

Open SNMP



Compare with Senegal, Angola, Tanzania, Ghana, Nigeria

Open SSDP



ASNs/ISPs in Senegal

So let's look at Senegal'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
- Senegal has 10 ASNs assigned to 4 Network Operators (most of whom are ISPs)
- And not all are equal…

Let us examine performance of best practice deployment of network equipment

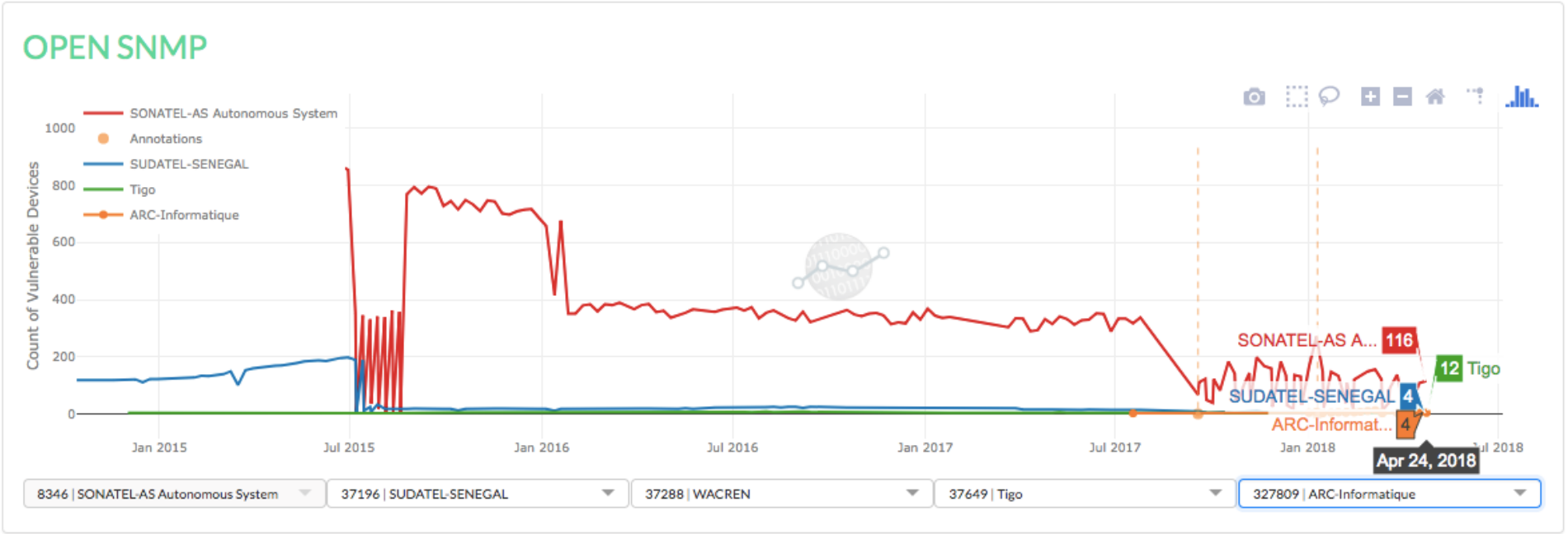
In each case let's ask:

- What has caused an improvement
- What has caused a worsening of "polluted" deployments

Comparison across 4 Senegalese ASNs
Open DNS

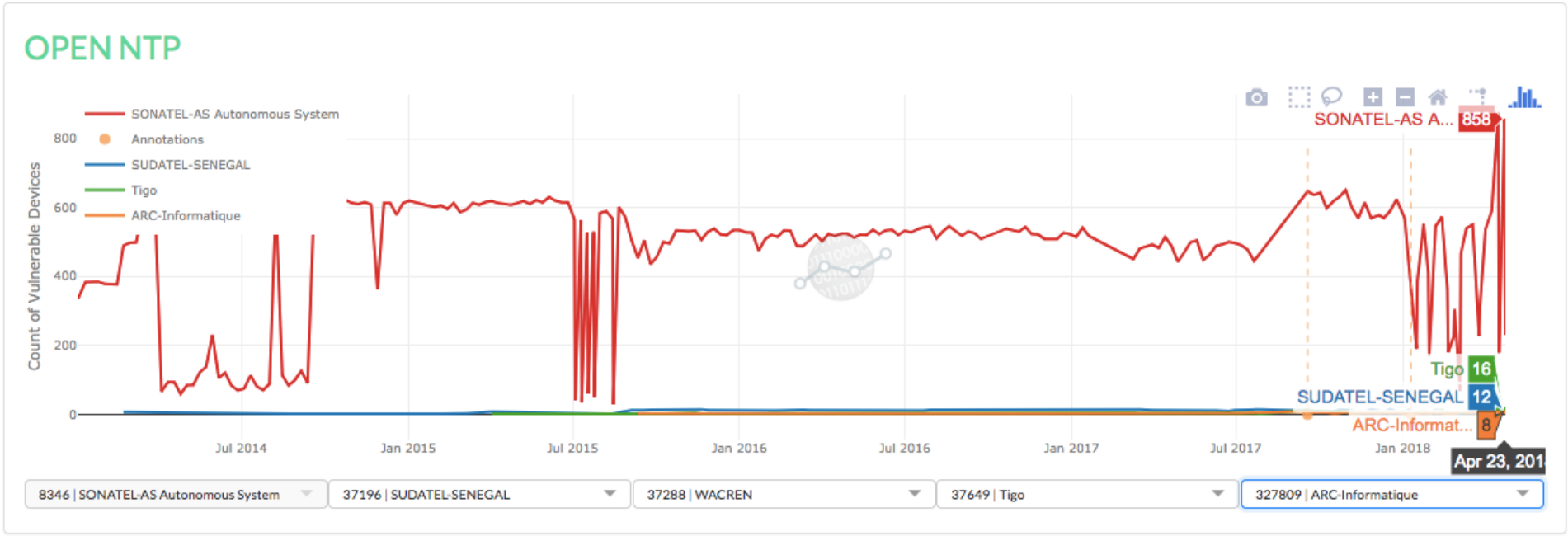
CyberGreen

Comparison across 4 Senegalese ASNs
Open SNMP



CyberGreen

Comparison across 4 Senegalese ASNs
Open NTP



CyberGreen

What can be done?


Download Open SSDP


Download Open NTP


Download Open DNS


Download SpamBot

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

Country level analysis report

CyberGreen

Country Report: Canada

Country Overview

Population: 36,290,000[1]

Area: 9,984,700 sq km[1]

GDP: $1,529.76 billion[1]

Autonomous Systems: 1,899[2]

Internet Service Providers: 44[3]

IPv4: ~76 million

Introduction

CyberGreen seeks to improve cyber health through research, metrics and outreach. Our modern economy is highly dependent on the Internet, which itself is dependent on information and network security. Threats to the Internet's security and stability can have effects on the global economy.

Only via repeatable measurements can we identify risks to global cyber health and address these. CyberGreen makes measurement data available to remediation teams, policymakers, CERTs and CyberGreen's users so that they can take collective action on it.

CyberGreen will achieve this by conducting weekly internet-wide scans of publicly accessible IPv4 hosts, in search of open DNS, SNMP, SSDP and NTP servers. If left unmitigated, these open servers can be used as infrastructure for launching *Distributed Denial of Service* (DDoS) attacks by malicious actors. Any DDoS attack has hundreds of victims – the target, and the hundreds of owners whose resources are hijacked for the attack.

Attackers are continuously improving their craft. Ten years ago, resources combined into networks of controlled *bots*. Now, attackers use *reflectors* – legitimate servers that are tricked into sending traffic to a target.

CyberGreen's mission is to encourage various stakeholders, using robust data and metrics, to take efforts to mitigate the risks that are presented in this report. The ultimate goal is a healthier Canadian Cyber Ecosystem which, in turn, leads to a healthier global Cyber Ecosystem.

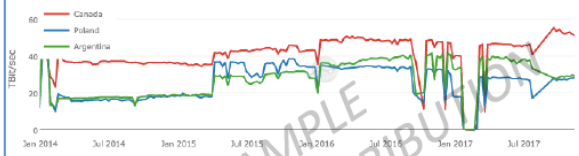
1 World Bank 2016
2 http://stats.cybergreen.net/asn
3 https://en.wikipedia.org/wiki/List_of_internet_service_providers_of_Canada

CyberGreen

Country Report: Canada

Country Comparison

With respect to its global standing, Canada's cyber health state can be further contextualized by doing a comparison against other countries with similarly-sized populations. For this analysis, a comparative analysis has been conducted between Canada, Argentina, and Poland.



Country	Open Recursive DNS	Open NTP	Open SNMP	Open SSDP	DDOS Potential TBit/sec	DDOS Rank
Canada	115,622	80,480	23,000	49,950	51	13
Argentina	50,358	26,401	21,215	413,236	30	17
Poland	108,461	41,924	20,014	12,913	28	18

As the graph and numbers above show, Canada has a higher DDOS exposure score relative to Argentina and Poland. This result is largely driven by the larger number of NTP servers that Canada operates. NTP is an infrastructural protocol, and has a high amplification factor, making it an attractive reflector. Canada likely operates this large NTP infrastructure as a side effect of their large population of cloud providers, a function of being a wired and wealthy country with a mature Internet infrastructure.

The high SSDP number in Argentina may correlate with its relatively young Internet infrastructure, although more analysis of Argentina would need to be done to concretely reach a conclusion on this. Regardless, recommendations for focused mitigation efforts would look different in Canada and Argentina given the numbers seen in the table.

Mitigation, therefore, is not necessarily a "one size fits all" approach and requires a needs analysis like this to better understand the areas of improvement 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.

CyberGreen

Country Report: Canada

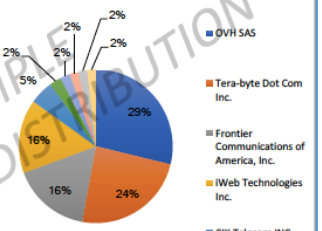
ISP Analysis

CyberGreen performs internet scans and collects and analyzes data for four open recursive protocols (NTP, DNS, SSDP, SNMP) commonly used to execute DDoS reflection attacks.

The following rankings and charts provide insight into the Canadian ISPs that host the greatest number of those open recursive protocols. CyberGreen ranks the top 20 ISPs that host these protocols. The top 10 are visualized in a pie chart.

Major DNS Contributors

Rank	ISP	Count Type
1	OVH SAS	18947 Cloud
2	Tera-byte Dot Com Inc.	15816 Cloud
3	Frontier Communications of America, Inc.	10858 Telco
4	iWeb Technologies Inc.	10239 Cloud
5	CIK Telecom INC	3291 Telco
6	Netelligent Hosting Services Inc.	1614 Cloud
7	Bell Canada	1354 Telco
8	Radiant Communications Canada Ltd.	1233 Cloud
9	GloboTech Communications	1225 Cloud
10	Shaw Communications Inc.	1178 Telco
11	Rogers Cable Communications Inc.	1036 Telco
12	Softcom Technology Consulting Inc.	886 Cloud
13	TELUS Communications Inc.	857 Telco
14	Videotron Telecom Ltee	756 Telco
15	Idigital Internet Inc.	717 Cloud
16	DISTRIBUTEL COMMUNICATIONS LTD.	708 Telco
17	Internet Access Solutions Ltd.	627 Cloud
18	TeraGo Networks Inc.	566 Cloud
19	Egate Networks Inc.	544 Cloud
20	MTS Inc.	464 Cloud



The rankings in the figure above can be used by policymakers and network operators to launch a targeted mitigation campaign with the cooperation of highly ranked ISPs.

Of the 4 open protocols that are scanned by CyberGreen, DNS is the most prevalent of those risks in Canada. Of the 115,000+ open DNS servers nationwide, over half of them are hosted by the top 5 organizations listed above. The providers listed are primarily dominated by colocation and cloud services, implying some degree of centralized management and the potential for solutions such as BCP38.

Furthermore, among the top 10 highest contributors to Open DNS, the top 5 ISPs host 90% of open recursive DNS servers. Collaboration and cooperation among these 5 ISPs, national regulators, policymakers, and other stakeholders could result in a substantial reduction of potential DDoS infrastructure.

CyberGreen

The public policy challenge

Market failures are resulting in network operators and device manufacturers not being incentivized to ensure improved cyber security practices in their operations.

The result is a large global base of vulnerable computers, modems/routers and Internet of Things devices which can be manipulated by Cyber criminals.

Communications regulators and/or CERTS should:

Utilize publicly available data on network risk indicators to engage ISPs to encourage better device deployment processes and operational decisions.

Encourage the adoption of the Internet Society's Mutually Agreed Norms for Routing Security, or MANRS (https://www.manrs.org) by network operators.

CyberGreen

Thank you!

Yurie Ito

yito@cybergreen.net