



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**.



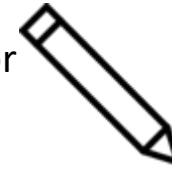
Provide a clearinghouse for  
Risk Mitigation BCPs.



Advocacy



Conduct weekly Internet  
scans for risk condition data



Capacity Building  
needs analysis and  
impact measurement



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

## Sponsors



## Collaborators



# Recognized as Global Good Practice

presented at GFCE / GCCS conference in New Delhi

<https://www.thegfce.com/good-practices/incident-capture-and-analytics>



Global Good Practices

November 2017

**diplo**

**GFCE**  
Global Forum on Cyber Experts

Practice: **Establish a clearinghouse for gathering systemic risk conditions data in global networks**

#Clearinghouse

We assess our personal health based on the tests we receive from doctors. Cybersecurity is like public health. CERTs and operators have trusted data — regularly updated about weaknesses in our networks, this helps them identify vulnerabilities, preserve cyber-health, and prevent incidents.

Related thematic areas:



Research and development



Cooperation and community building

Of particular interest to:



PRIVATE SECTOR

## Description

Internet networks are replete with systemic vulnerabilities. CERTs and other trusted operators require reliable information about their network's health over time. Various organisations have set up systems to scan networks for vulnerabilities and/or monitor cyber-attacks. Many of these sources are open, but their provenance and collection processes are often opaque. To acquire a truly satisfactory picture of the Internet's behaviour, a clearinghouse is needed that does not simply collect data, but leverages its collections to improve the process.

The clearinghouse collects raw data from multiple sources and processes it, in order to feed into Internet health metrics. Data is collected from carefully selected comprehensive data sources, and processed to ensure it is accurate and extensive, and its biases understood and addressed. It can then be analysed and contextualised to produce reliable metrics about how healthy the Internet is.



## Actors (or who this is for)

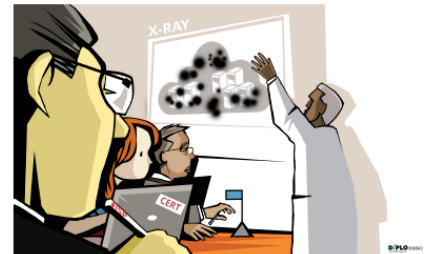
The clearinghouse produces quality data sources that can be used by CERTs, top-level ISPs, and national infrastructure organisations, as well as skilled technical departments within companies or organisations, and regulators to track the health of the ecosystem and suggest improvements. It also allows them to use the clearinghouse's aggregated data along with local proprietary data to generate their own statistics to measure and track the ecosystem's health.

Researchers from multiple communities — academia, CERTs, and industry — are also involved. They can both benefit from the quality data sources for their research work.

## Description

Statistically mature and vetted metrics, rather than raw data, should be presented to the parties in charge of keeping the network clean. The development and application of statistical methods to data allows for measurement and contextualisation of key indicators of malicious activity and risk conditions. Metrics should be normalised transparently, so that users can interpret and use the data in their own way.

A statistics platform, featuring metrics and data visualisation, allows for the measurement of key indicators of malicious activity and risk conditions, and enables analytical insight about patterns, priorities, and trends for action. Such intelligence can be used by the CERT/CSIRT community, security sector, corporations, and organisations. If the metrics are regularly published in reports about the health of the cyber-ecosystem and the mitigation impact, the decision-making level — including CEOs and government ministers — could become more aware and ready to act.



## Actors (or who this is for)

Everyone can benefit from obtaining trusted, clear, comprehensible data about the health of cyberspace:

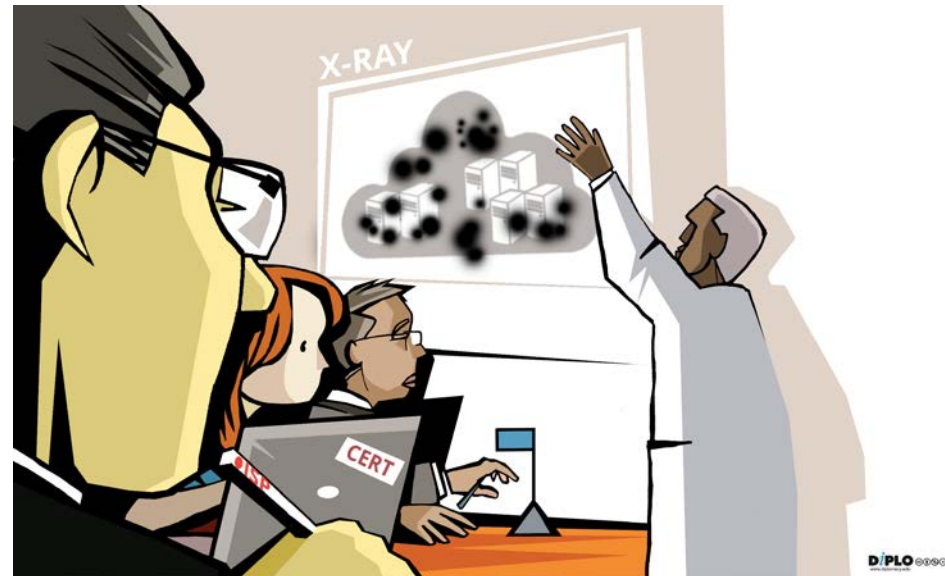
- CERTs can use it to enhance the trust of their partners, to prepare situational awareness, and to issue early warnings.
- Network operators are expected to monitor the conditions of their networks and act accordingly. Clear metrics can assist them in identifying risks and trends.
- Security departments in companies, institutions, and organisations can likewise benefit from receiving clear metrics on trends in their environment.

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

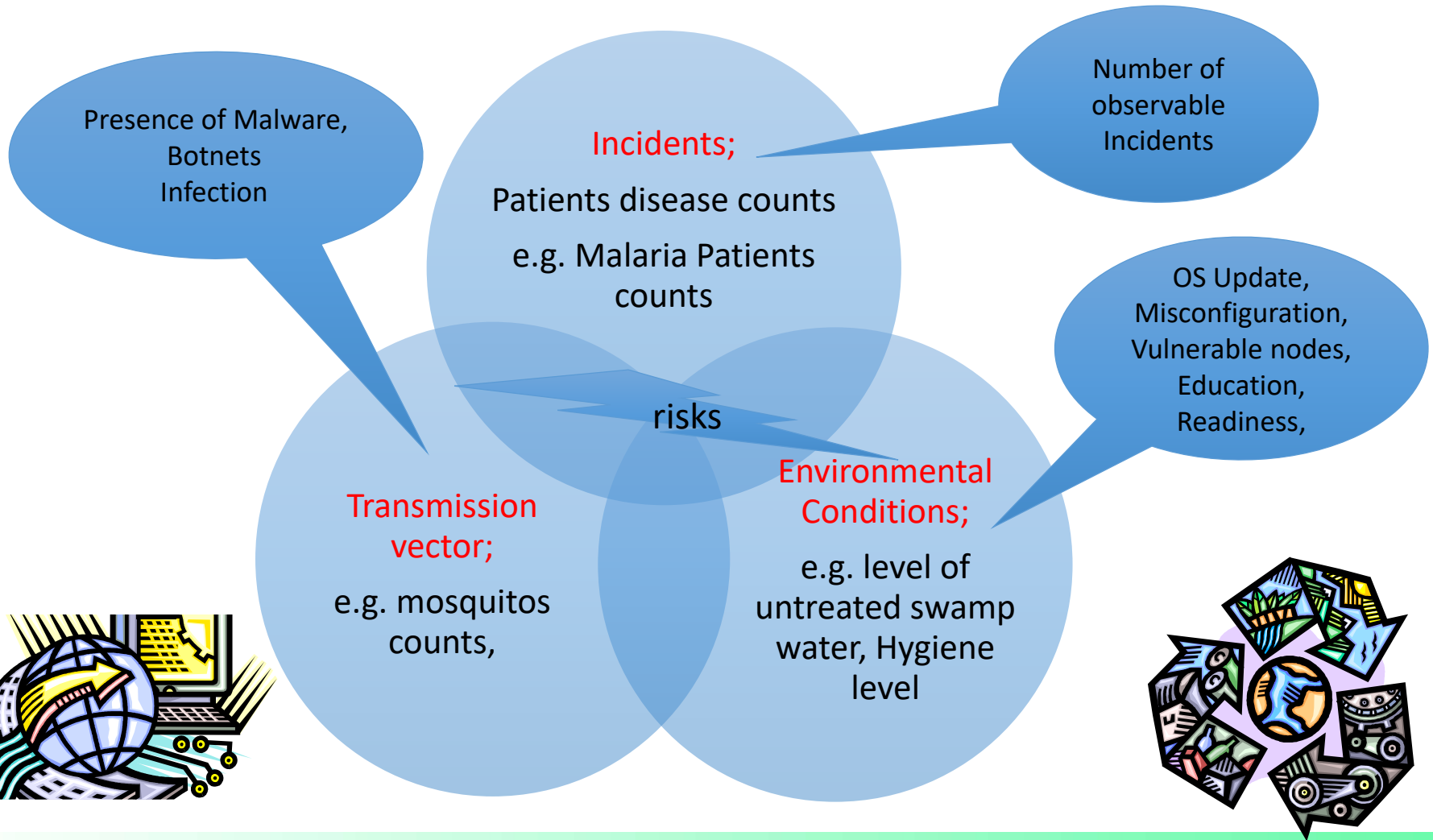
# Key Questions

---

- Do you know the state of your cyber ecosystem health of your country?
- Do you know how to improve it? And it's impact?



# 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 International public health security: a global network of national health systems and technical partners, focused on four major areas of work, coordinated by WHO



The screenshot shows the CDC website for Ebola (Ebola Virus Disease). The header includes the CDC logo and the text 'Centers for Disease Control and Prevention CDC 24/7: Saving Lives. Protecting People™'. Below the header are navigation options: 'MENU', 'CDC A-Z', and 'SEARCH'. The main heading is 'Ebola (Ebola Virus Disease)'. There are social media icons for Facebook, Twitter, and a plus sign, and a language dropdown menu set to 'English'. The main content area features a large banner with the text 'Top 10 Things You REALLY Need to Know about EBOLA'. Below the banner is a slide titled 'You can't get Ebola from a handshake or a hug.' with a large number '1' and an illustration of two people shaking hands. Below the slide are two columns of text: 'SIGNS AND SYMPTOMS' and 'FOR HEALTHCARE WORKERS'. The right sidebar contains the text '2014 West Africa Outbreak' and a paragraph describing the epidemic, followed by a link to 'Latest CDC Outbreak Information' and the date 'Updated October 27, 2015'.

# CyberGreen: What we measure

Type	Description
Open DNS	Domain Name System (DNS) is a standard protocol that translates human-friendly host names like <code>www.cybergreen.net</code> into numerical, Internet Protocol (IP) addresses such as <code>197.222.126.114</code> . 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.



# 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

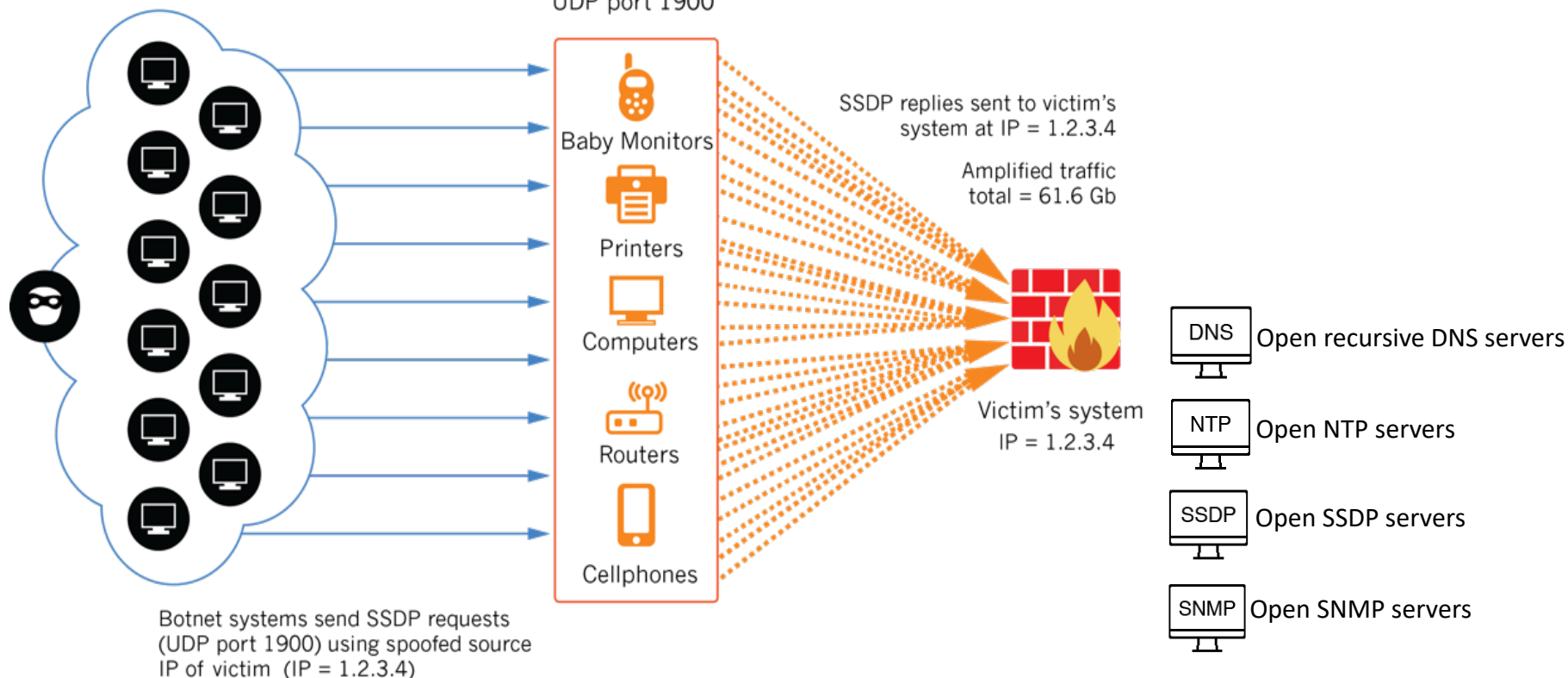


# Abuse-able systemic conditions posing risks to others \*including to yourself\*

## SSDP Amplification Attack

Attacker controlled botnet targets victim's system with IP = 1.2.3.4

UPnP-enabled devices open to the Internet on UDP port 1900



Total size of all requests = 2 Gb

# DDoS attack against DynDNS

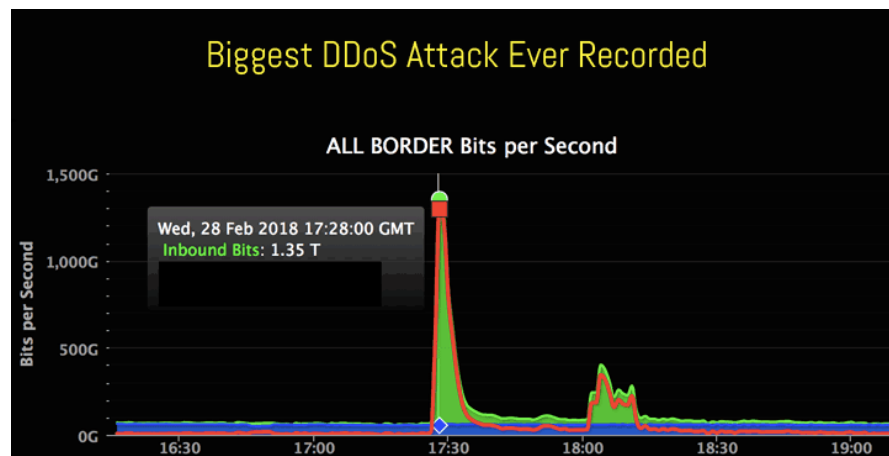
## October 21, 2016

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

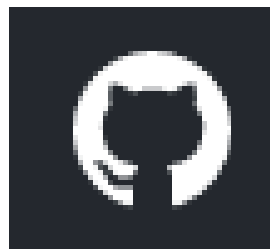


The screenshot shows a web browser displaying a blog post from Dyn. The page header includes the Dyn logo and navigation links for PRODUCTS, RESOURCES, SUPPORT, and COMPANY. Below the header, there are additional navigation links: Home, Blog, Topics, Whitepapers & eBooks, Case Studies, Webinars, Video, and Analyst Reports. The main content area features a breadcrumb trail: Home > Dyn Blog > Dyn Statement on 10/21/2016 DDoS Attack. The article title is "Dyn Statement on 10/21/2016 DDoS Attack". It includes social media sharing icons for LinkedIn (1,882), Facebook (5,041), and Twitter (958). The post is dated October 22, 2016, and is attributed to Kyle York. The text of the post begins with: "It's likely that at this point you've seen some of the many news accounts of the Distributed Denial of Service (DDoS) attack Dyn sustained against our Managed DNS infrastructure this past Friday, October 21. We'd like to take this opportunity to share additional details and context regarding the attack. At the time of this writing, we are carefully monitoring for any additional attacks. Please note that our investigation regarding root cause continues and will be the topic of future updates. It is worth noting that we are unlikely to share all details of the attack and our mitigation efforts to preserve future defenses." The post also includes a list of two points: 1. Acknowledging the tremendous efforts of Dyn's operations and support teams in doing battle with what's likely to be seen as a historic attack. 2. Acknowledging the tremendous support of Dyn's customers, many of whom reached out to support our mitigation efforts even as they were impacted. Service to our customers is always our number one priority and we appreciate their understanding in an

# 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

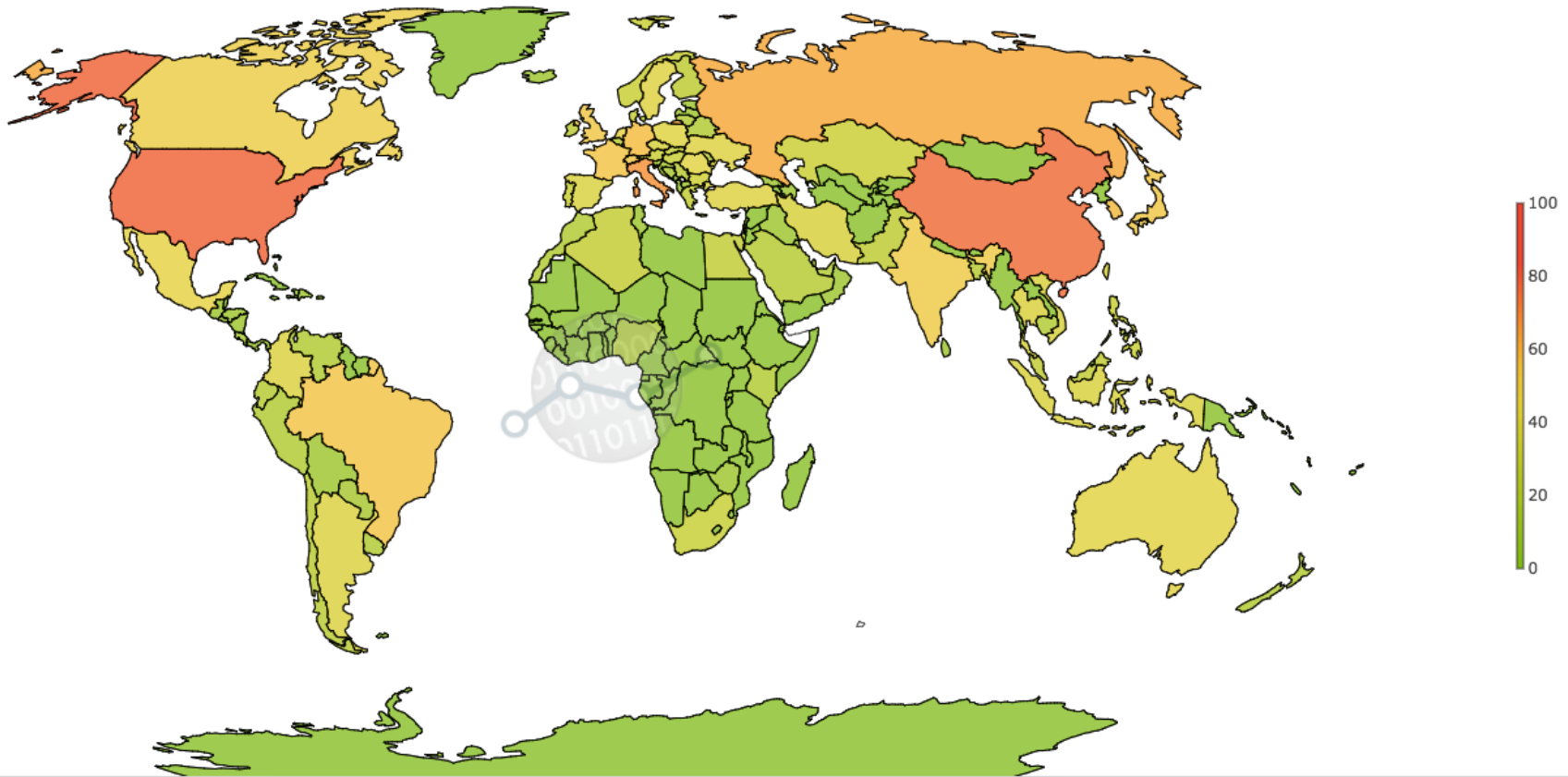
- Network service interrupted
- Isolation of victim network by network providers from the rest of Internet to mitigate collateral damage to other customers

## Financial

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

# Global View

<http://stats.cybergreen.net>





# Senegal Overview

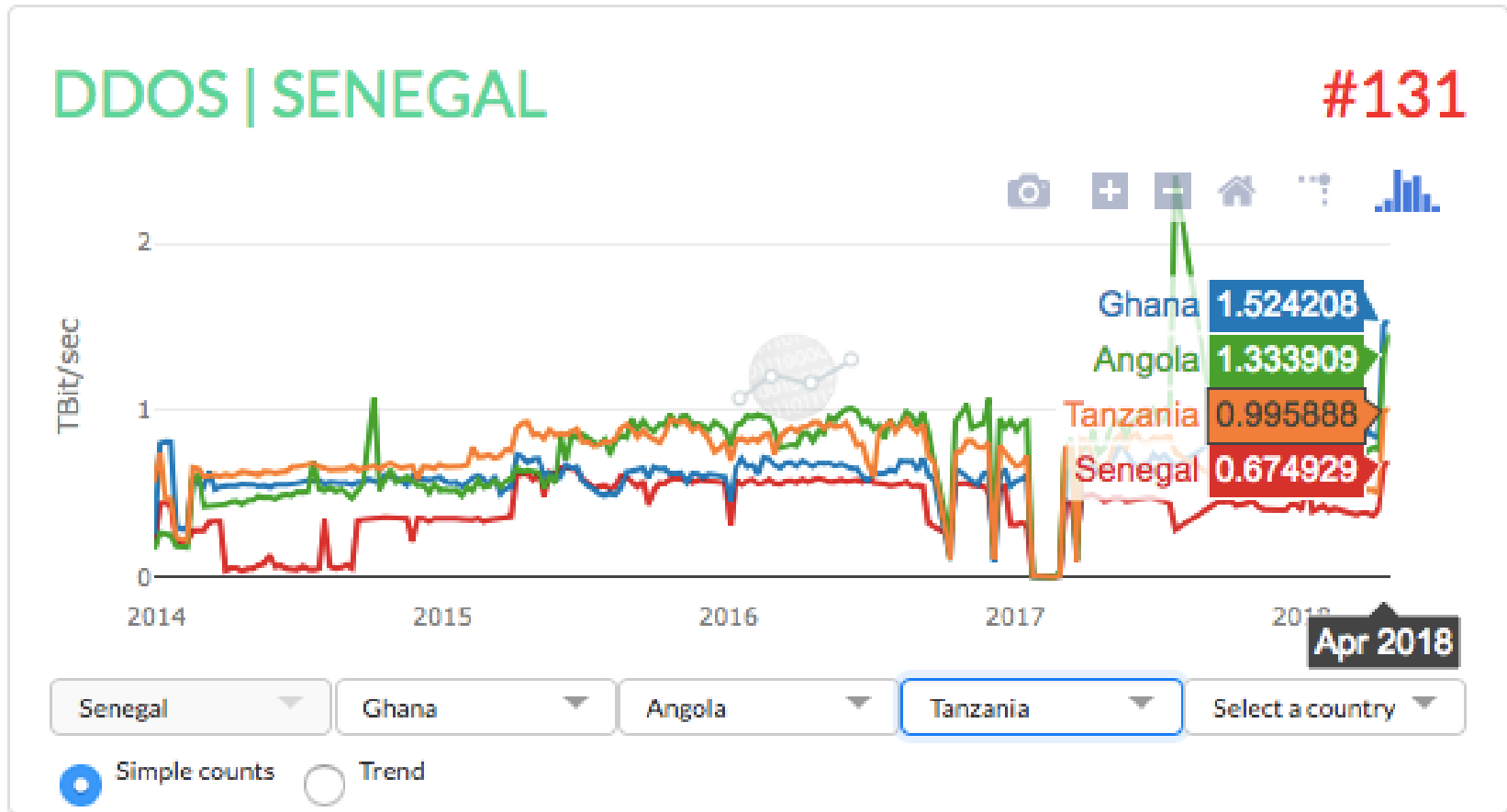
Week of April 23, 2018 – April 29, 2018

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



# A note on methodology

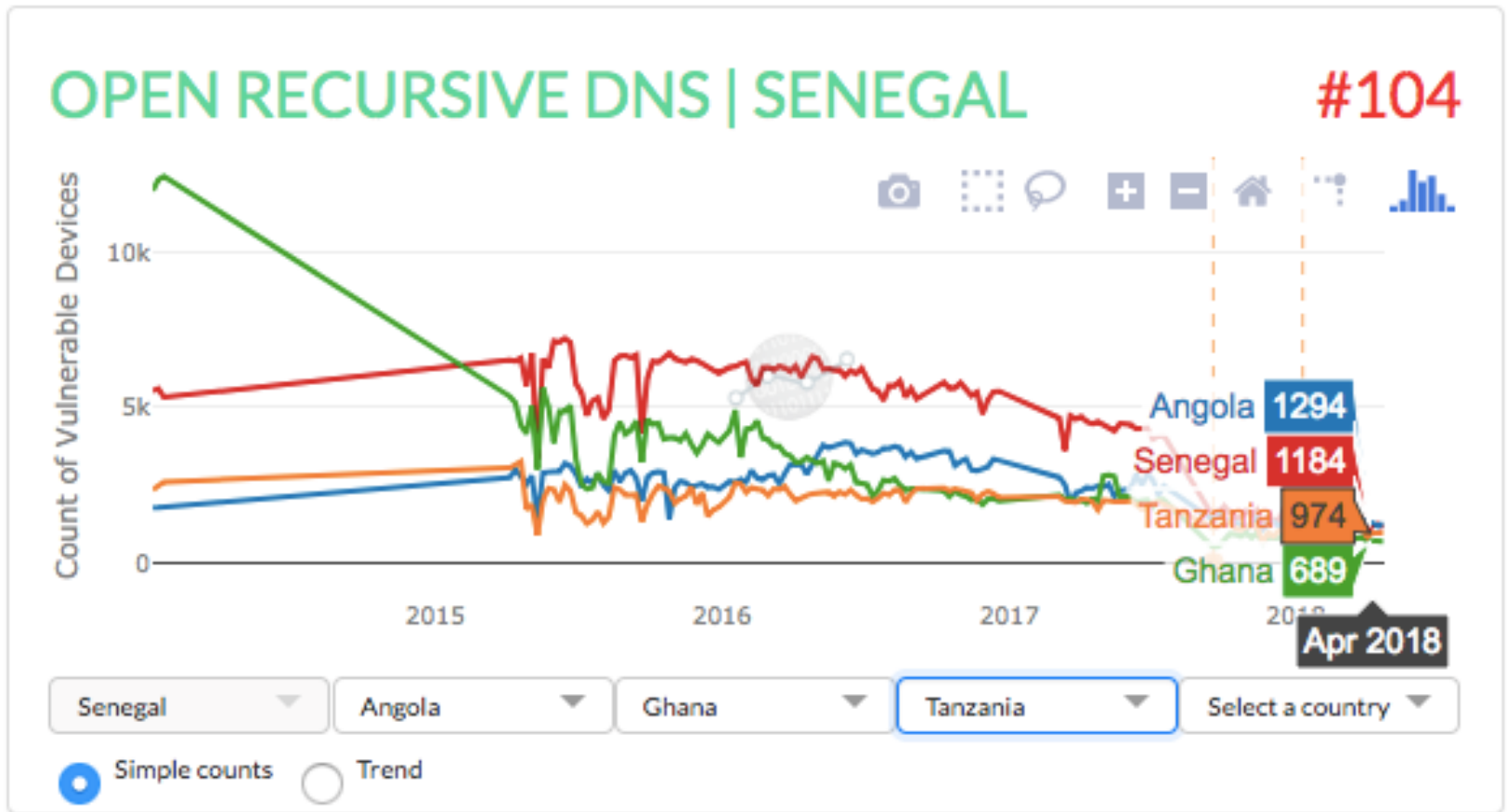
---

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.*

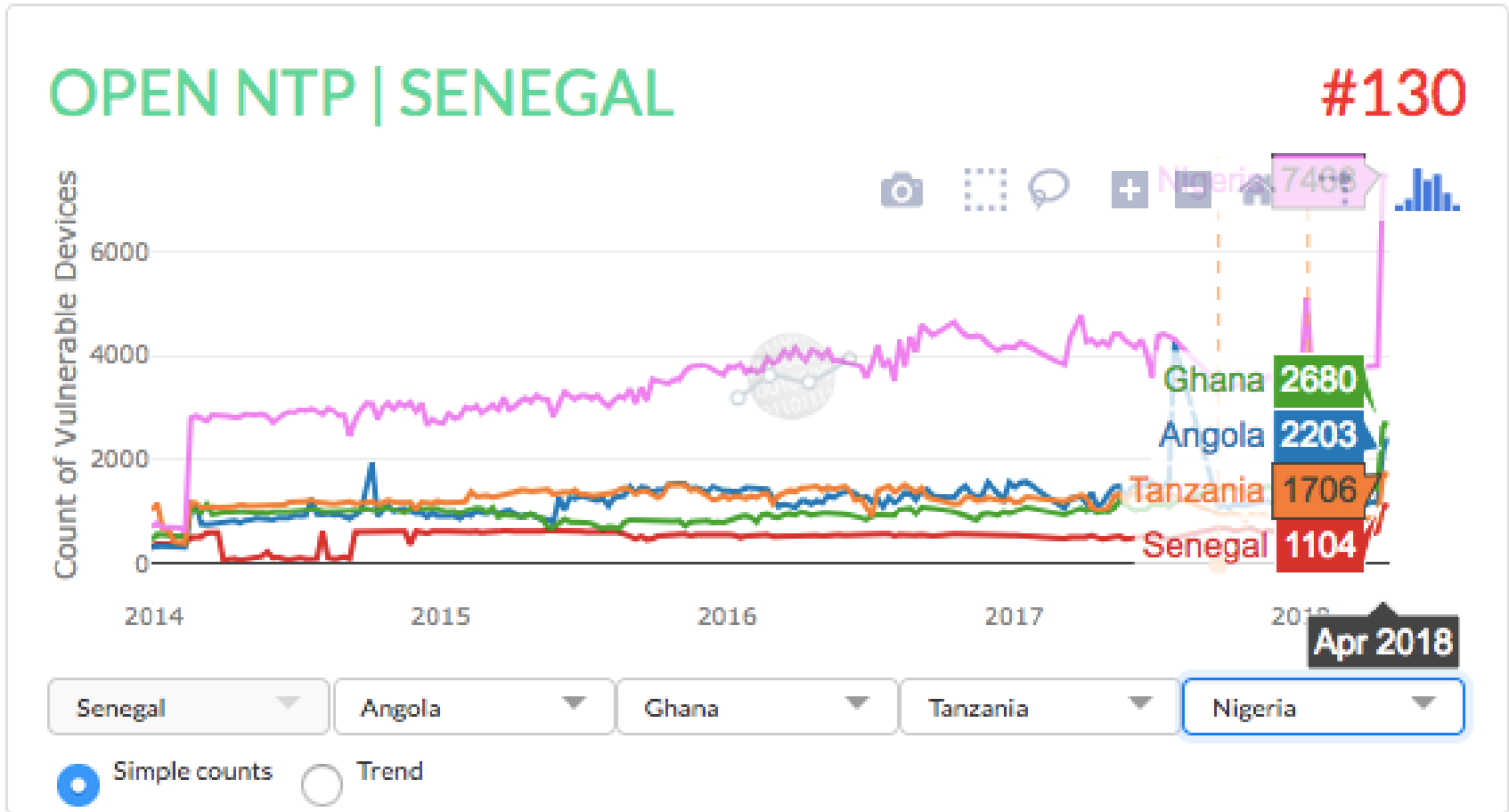
# Compare with Senegal, Angola, Tanzania, Ghana

## Open DNS



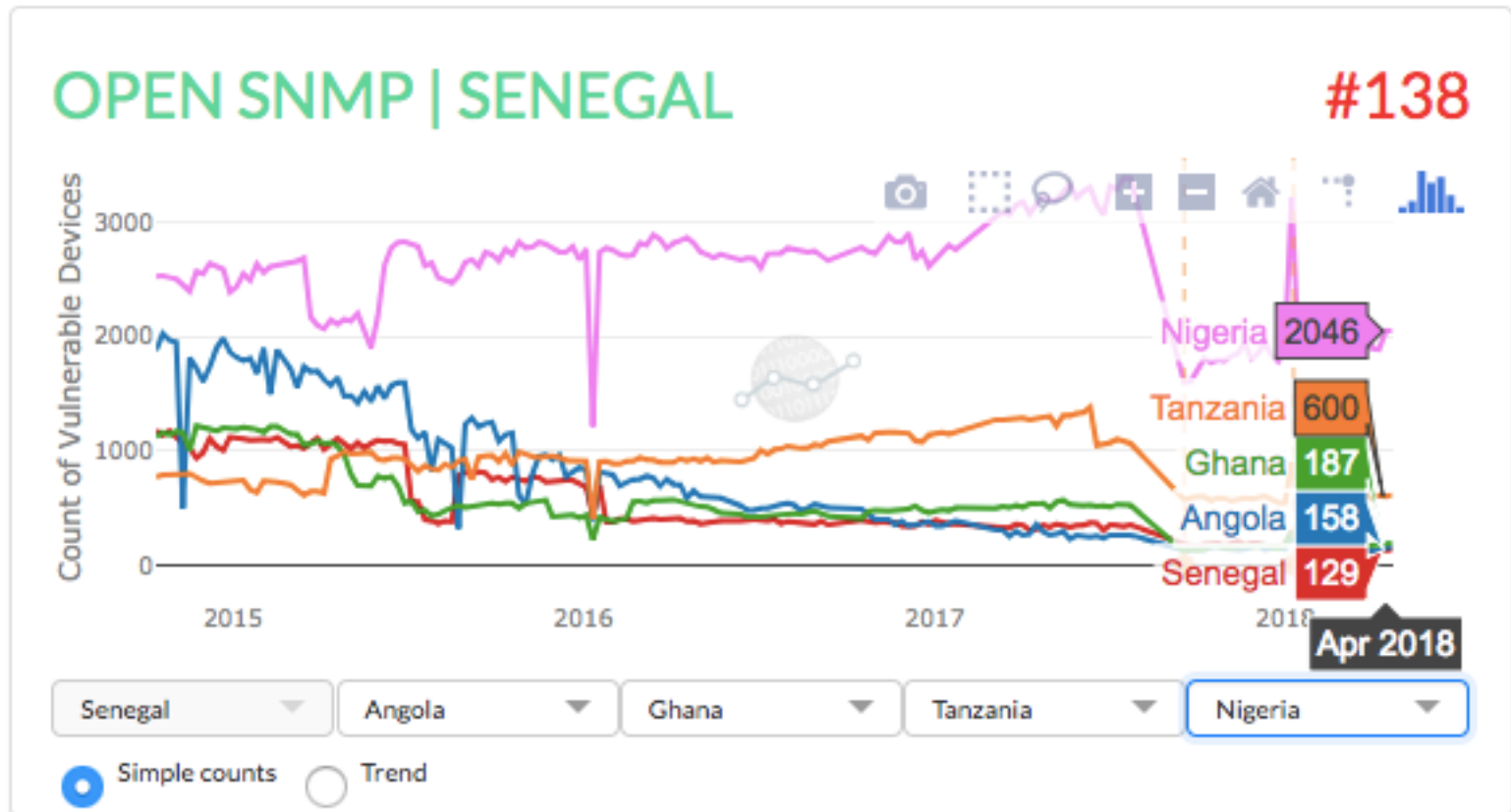
Compare with Senegal, Angola, Tanzania, Ghana, Nigeria

# Open NTP



Compare with Senegal, Angola, Tanzania, Ghana, Nigeria

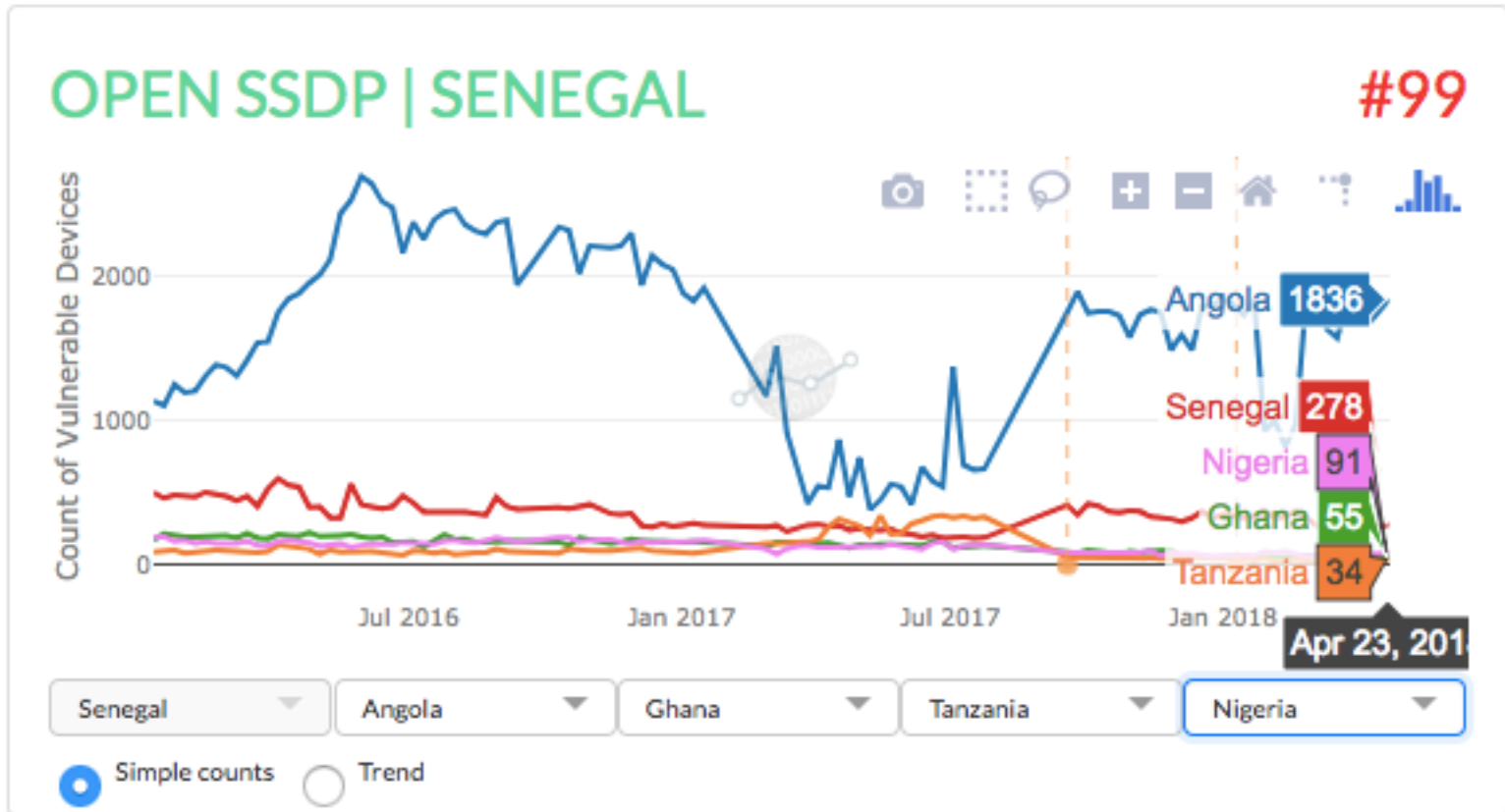
# Open SNMP





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

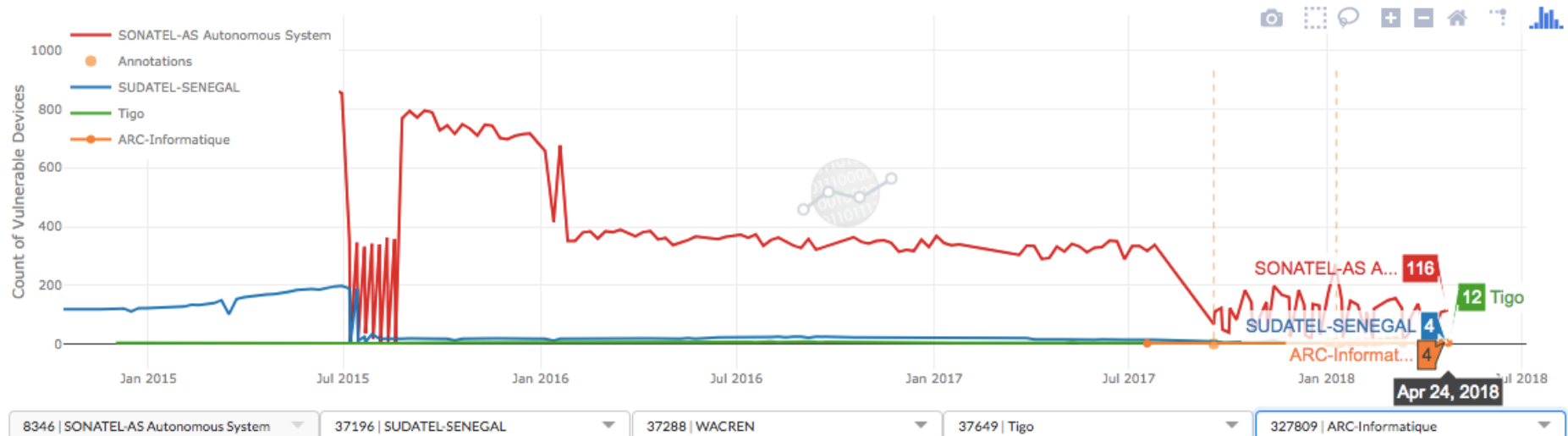
## OPEN RECURSIVE DNS



# Comparison across 4 Senegalese ASNs

## Open SNMP

### OPEN SNMP

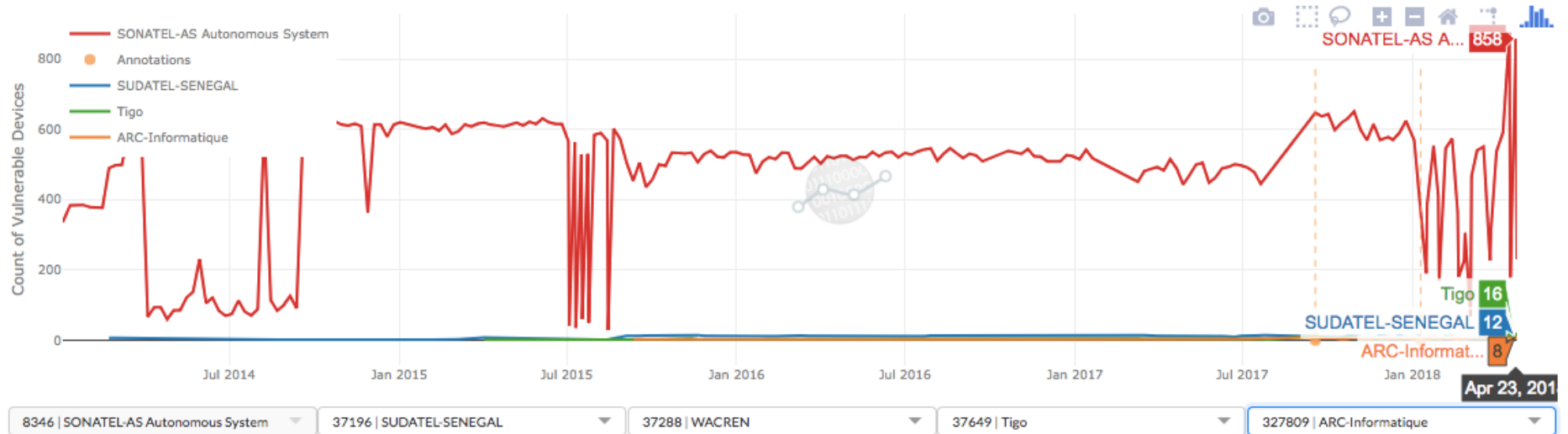




# Comparison across 4 Senegalese ASNs

## Open NTP

### OPEN NTP



# What can be done?

---



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



## Country Overview



Population: 36,290,000<sup>1</sup>  
 Area: 9,984,700 sq km<sup>1</sup>  
 GDP: \$1,529.76 billion<sup>1</sup>  
 Autonomous Systems: 1,899<sup>2</sup>  
 Internet Service Providers: 44<sup>3</sup>  
 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.

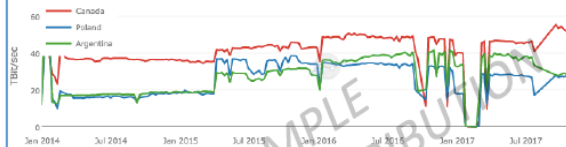
CyberGreen's mission is to encourage various stakeholders, using robust data and metrics, to take efforts to mitigate the risks that are presented in this report. The ultimate goal is a healthier Canadian Cyber Ecosystem which, in turn, leads to a healthier global Cyber Ecosystem.

<sup>1</sup> World Bank 2016  
<sup>2</sup> <http://data.asnregistry.com/>  
<sup>3</sup> [https://en.wikipedia.org/wiki/List\\_of\\_Internet\\_service\\_providers\\_of\\_Canada](https://en.wikipedia.org/wiki/List_of_Internet_service_providers_of_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 Tbl/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.

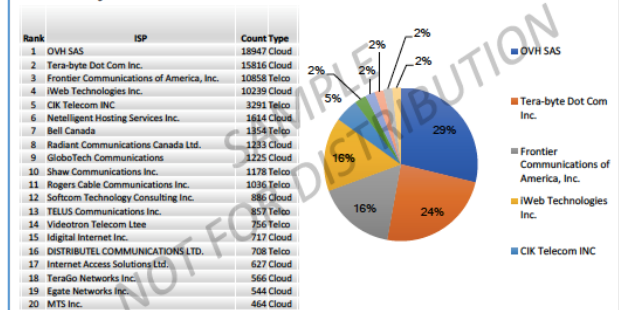


## ISP Analysis

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



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.



# 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.



Thank you!

Yurie Ito

[yito@cybergreen.net](mailto:yito@cybergreen.net)