Do we need IoT security?

Canadian Multistakeholder Process Enhancing IoT Security

iotsecurity2018.ca

cira
BUILDING A BETTER ONLINE CANADA

Jacques Latour, CTO
Canadian Internet Registration Authority

April 4, 2018

BUILDING A BETTER ONLINE CANADA

.CA

REGISTRY and **DNS**

2.7 million .CA

Cybersecurity Services

100,000 new cybersecurity threats blocked daily by D-Zone Firewall.

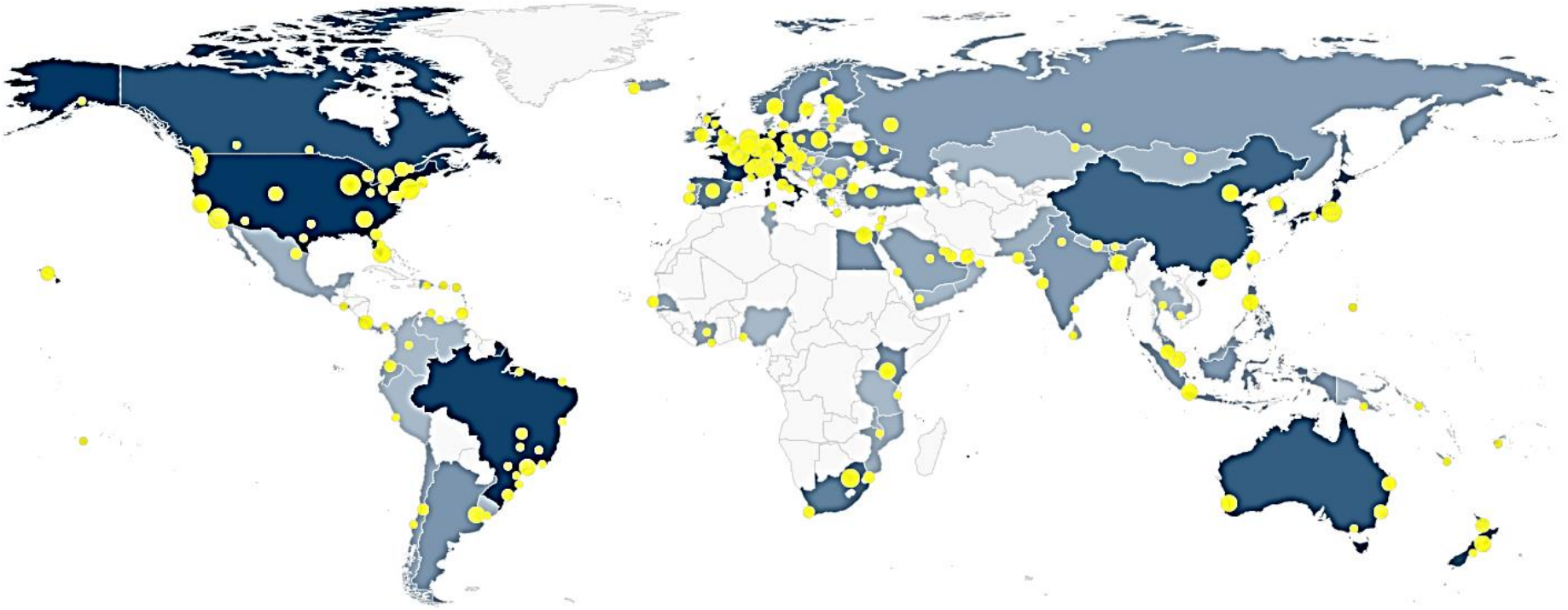
Registry Services

Robust top-level domain products and services.

We support initiatives that enhance Canadians' internet experience:

Global Internet Leadership	• Support internet governance and standards through global organizations such as ICANN and CENTR
Canadian Initiatives	• **11** Internet Exchange Points nation-wide • **280,000+** internet performance tests conducted last year
Community Initiatives	• More than **$4.2 million** in grants to **102** projects through our Community Investment Program

DNS ANYCAST SITE LOCATION (100s) FOR .CA DOMAIN NAME RESOLUTION



THE NEED FOR IoT SECURITY

- For many internet organizations, the #1 risk on their risk register is a large scale DDoS attack
- Ideal mitigation mechanisms for this risk is to prevent weaponization of IoT devices
  - Protect IoT devices from internet harm
  - Protect the internet from IoT attacks
- The **threat** that **IoT devices** bring is **scale**. The scale of million and billions of IoT device is the threat we need to mitigate.

IoT THREAT LANDSCAPE SPECIFIC TO THE INTERNET - **SCALE**

- Compromised IoT devices:
  - Used in internet attacks i.e. MEMCACHED, MIRAI Attack (DDoS) targeting DNS servers (+1 Tbs)
- IoT traffic generation, reflection and amplification
  - IoT device used to amplification traffic attack (DDoS) NTP, DNS, SNMP, (flavor of the day)
- The **scale** of IoT threat landscape and the breath of exploits is what need to mitigated
  - IoT devices must not have wide open internet access (protected by firewall)

IT'S REAL & JUST STARTING

MIRAI BOTNET