

## JANUARY

**Russia >>> 2 Hours**  
Penitentiary Service

## FEBRUARY

**Ukraine >>> Several Days**  
Security Service of Ukraine

## Russia >>> 1 Day

Russian National Guard (RosGvardiya)

## MARCH

**Philippines >>> 6 Hours**

Government Website

**China >>> 9 Hours**

Inter-Parliamentary Alliance Website

**Italy >>> 1 Day**

Italian Lower House of Parliament

## MAY

**Belgium >>> Several Hours**

My Minfin, the government's official tax- and form-filing portal

## JULY

**Russia >>> 1 Hour**

Russian Defense Ministry

**Ukraine >>> NA**

Defense Ministry Portal

## AUGUST

**Philippines >>> 3 Weeks**

Online Portal for Covid Vaccination

## SEPTEMBER

**Netherlands >>> 1 day**

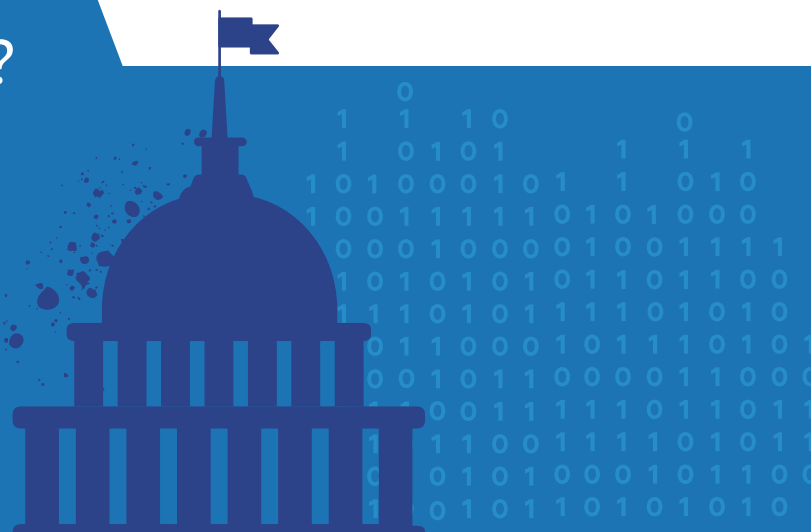
Ministry of Health (Corona Check System)

**New Zealand >>> 3-5 Days**

MetService, Inland Revenue and NZ Post

## Why Governments?

- Political Upheavals
- Ideological Belief
- Cyber Warfare
- Ulterior Motives
- Extortion



## The DDoS Problem for Governments

### 1 Increase

in complexity, volume, & velocity.

### 2 Less time

for current DDoS mitigation systems to react.

### 3 Penetrates

the best mitigation solutions.



## There is the need

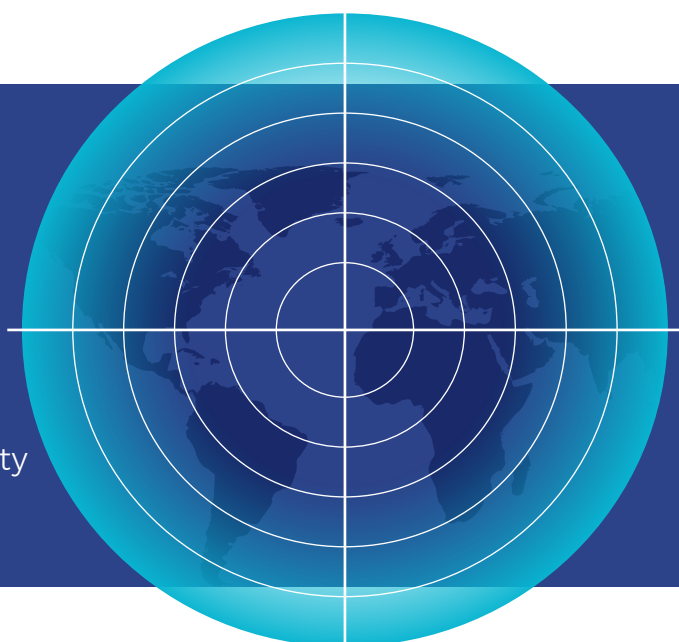
to detect and close all DDoS vulnerabilities on going, before an attack is launched.

Allowing mitigation solutions to respond in the fastest possible way with minimal manual intervention.

## About RADAR™

Working with any mitigation solution installed, RADAR™ offers superior DDoS coverage and automated DDoS protection.

RADAR™ simulates over 100 attack vectors with all public facing IPs 24/7, giving real time visibility to all DDoS vulnerabilities with zero downtime.



### Reference:

<https://bit.ly/3mO6bYk>

<https://bit.ly/3lxunPr>

<https://bit.ly/3BB04Np>

<https://bit.ly/3lyADX7>

<https://bit.ly/3BCdV5X>

<https://bit.ly/2YG0T9w>

<https://bit.ly/3lzKXhm>

<https://bit.ly/3lAgWyh>

<https://bit.ly/3BzgFBh>

<https://tass.com/society/1253013>

<https://tass.com/society/1245845>

<https://bit.ly/3v39X3S>