

National Computer Incident Response & Coordination Center of the Russian Federation



**ASEAN Regional Forum
March, 2019**

Legal Basis



**Federal Law № 187-FZ of July 26, 2017
«On Critical Information Infrastructure Security
of the Russian Federation»**



**FSS Order № 366 of July 24, 2018
«On National Computer Incident Response
& Coordination Center»**



Responsibility of NCIRCC

Domains: .ru, .su, .рф TLD

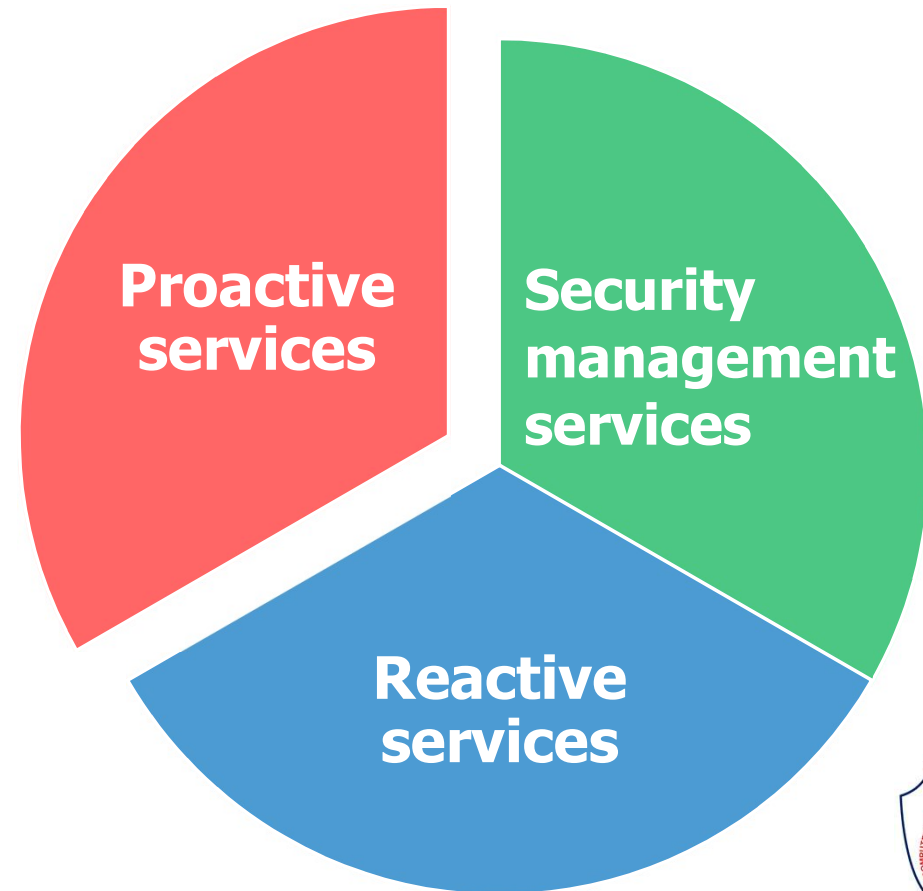
**IP address space physically located
in the Russian Federation**

**IP address space within jurisdiction
of the Russian Federation**



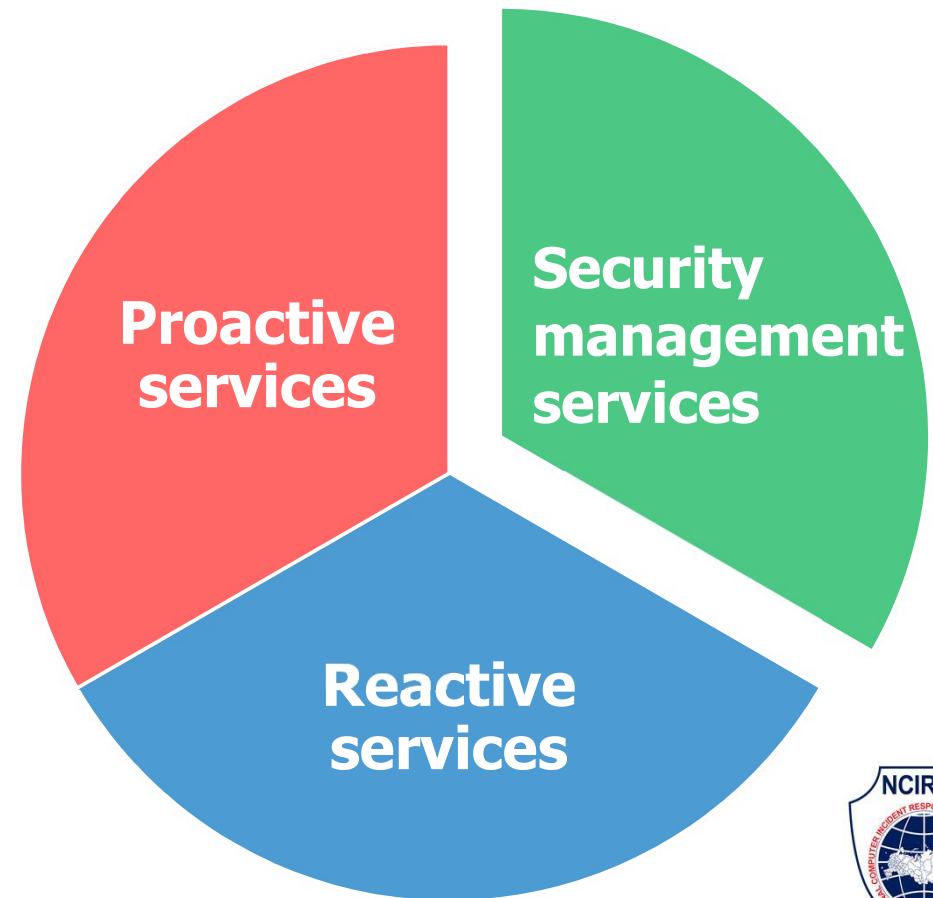
Services of NCIRCC

- Announcements
- Technology Review
- Security Audits or Assessments
- Configuration and Maintenance of Security Tools, Applications, and Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination



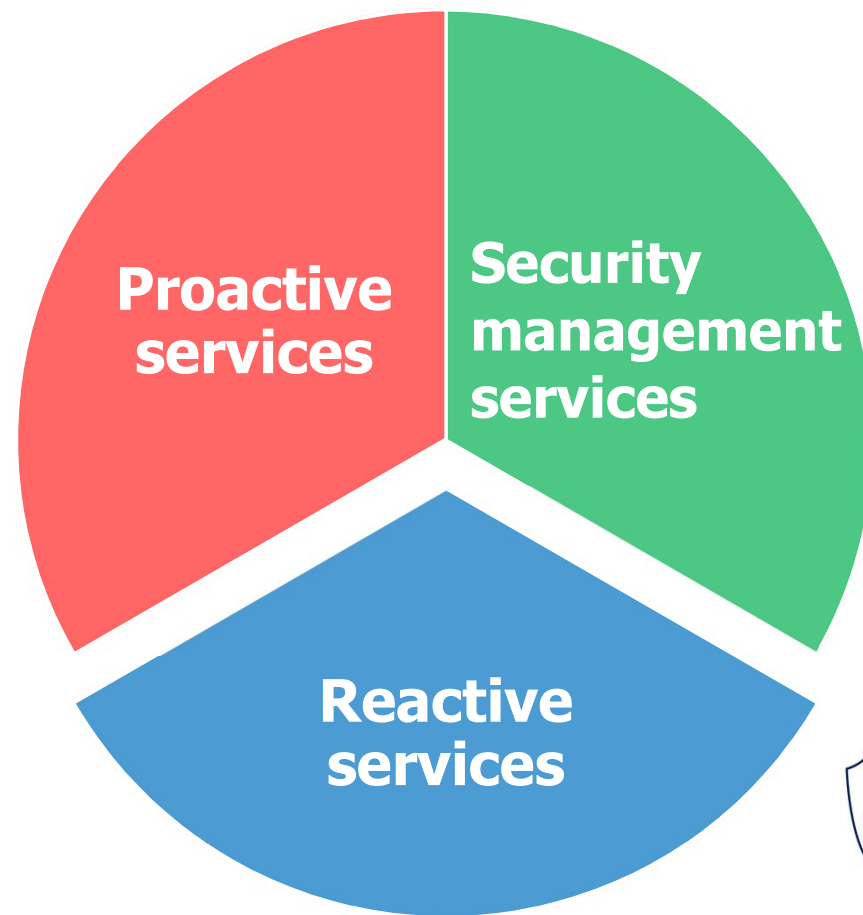
Services of NCIRCC

- Risk Analysis
- Security Consulting
- Awareness Building
- Education/Training



Services of NCIRCC

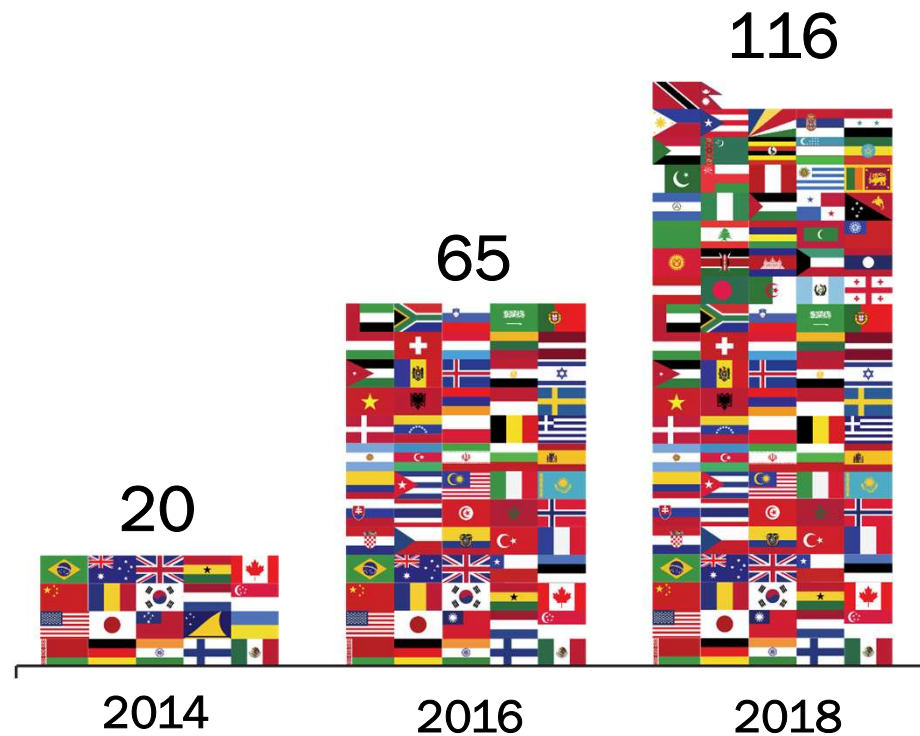
- Alerts and Warnings
- Incident Management
- Vulnerability Management
- Artifact Management



NCIRCC Cooperation

117

Foreign CERTs in 2019



Statistics of Cooperative Responses

In 2017 - **3000 sources**

In 2018 - **5700 sources**



Response to Attacks on Olympic Games Infrastructure in 2014



Canada



Malaysia



Thailand

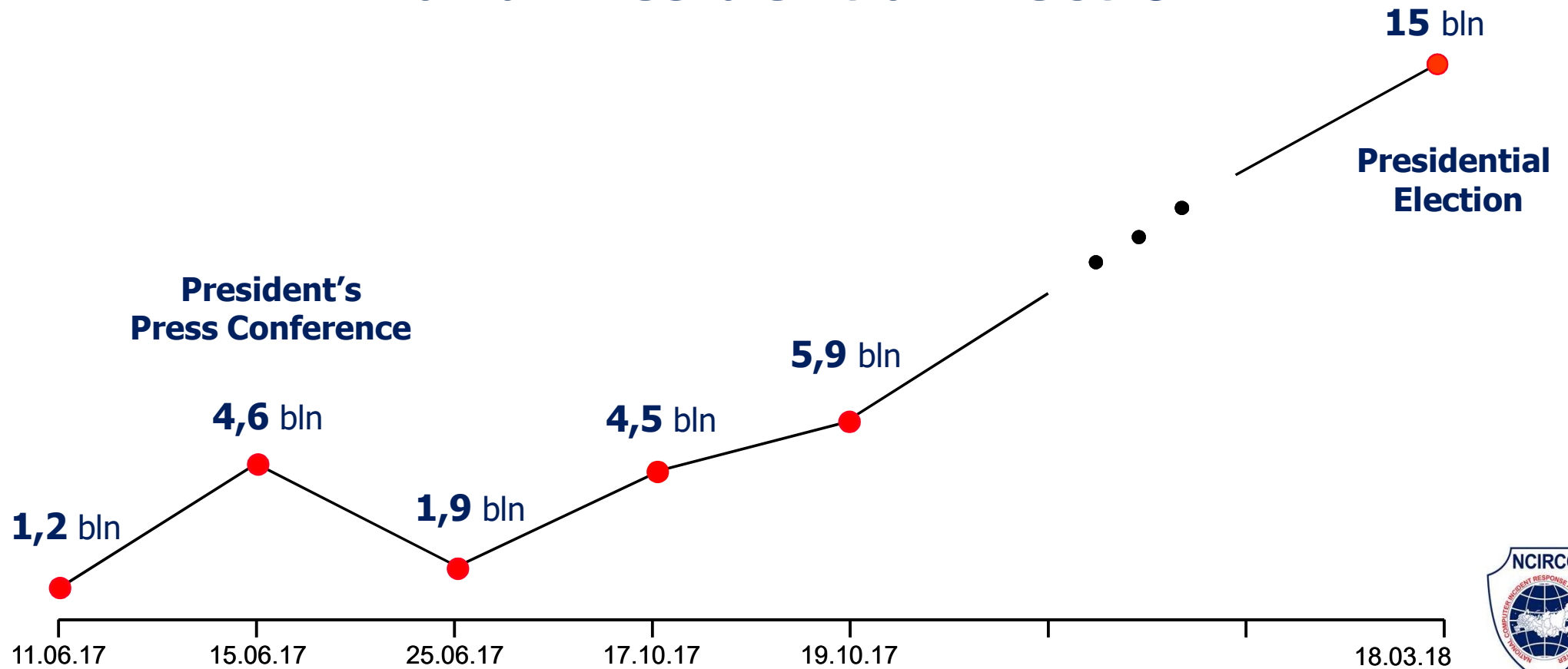


USA

**The C&C servers were disabled
within 3-24 hours**



Attacks during President's Press Conference and Presidential Election





Web: <http://cert.gov.ru>
E-mail: gov-cert@gov-cert.ru