Executive Agency "Electronic Communication Networks and Information Systems"

COMPUTER SECURITY INCIDENT RESPONSE TEAM

VASIL GRANCHAROV

DIRECTOR, CERT BG

www.esmis.government.bg

www.govcert.bg

REGULATORY FRAMEWORK

Electronic Governance Act;

Ordinance on General Requirements to Interoperability and Information Security;

Electronic Communications Act.

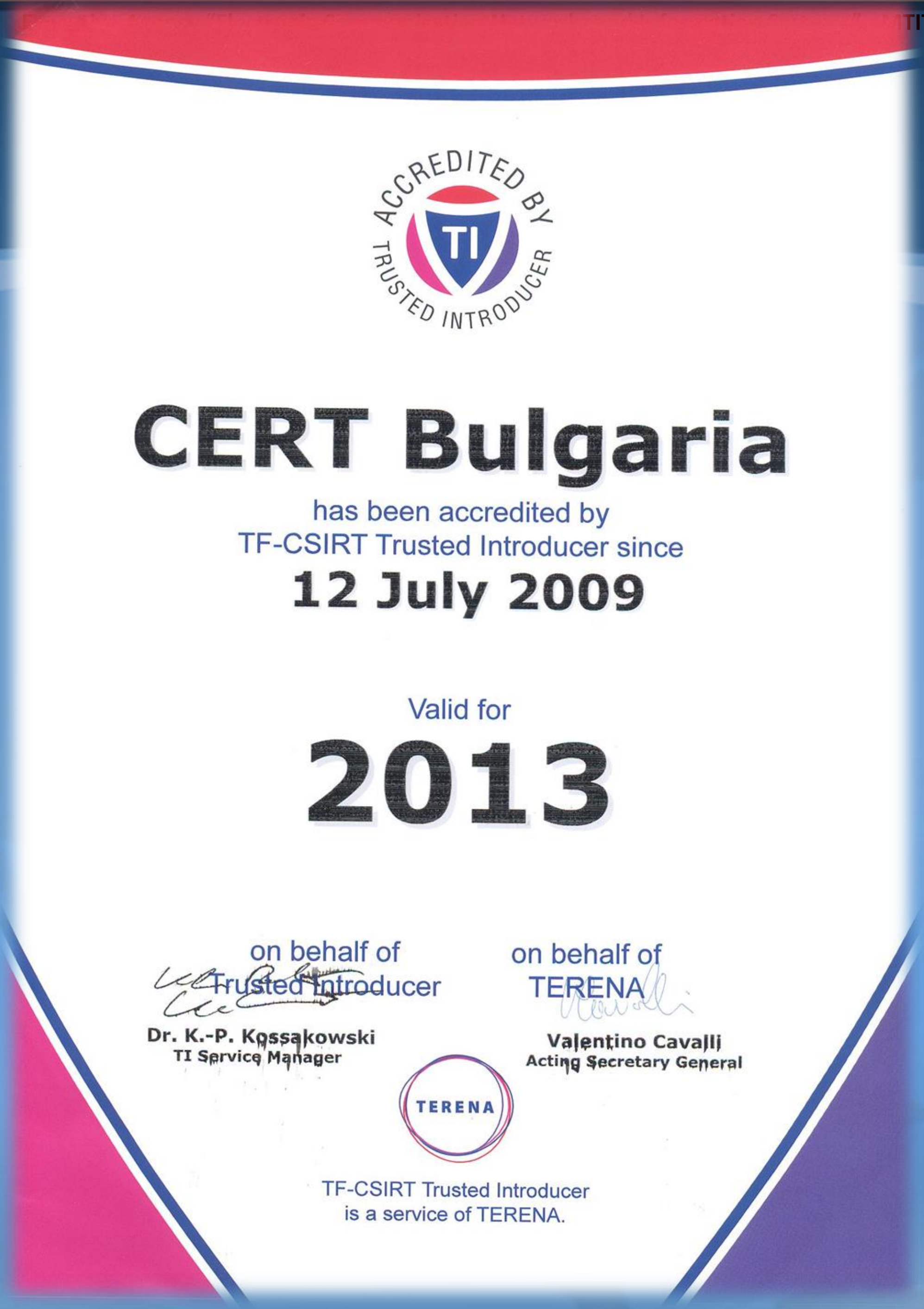
HISTORICAL OVERVIEW OF CERT BG

Established in 2008

ACCREDITED BY TRUSTED INTRODUCER

TI

First Trusted Introducer accreditation in 2009



ACCREDITED BY TRUSTED INTRODUCER

CERT Bulgaria

has been accredited by
TF-CSIRT Trusted Introducer since

12 July 2009

Valid for

2013

on behalf of
Trusted Introducer

Dr. K.-P. Kossakowski
TI Service Manager

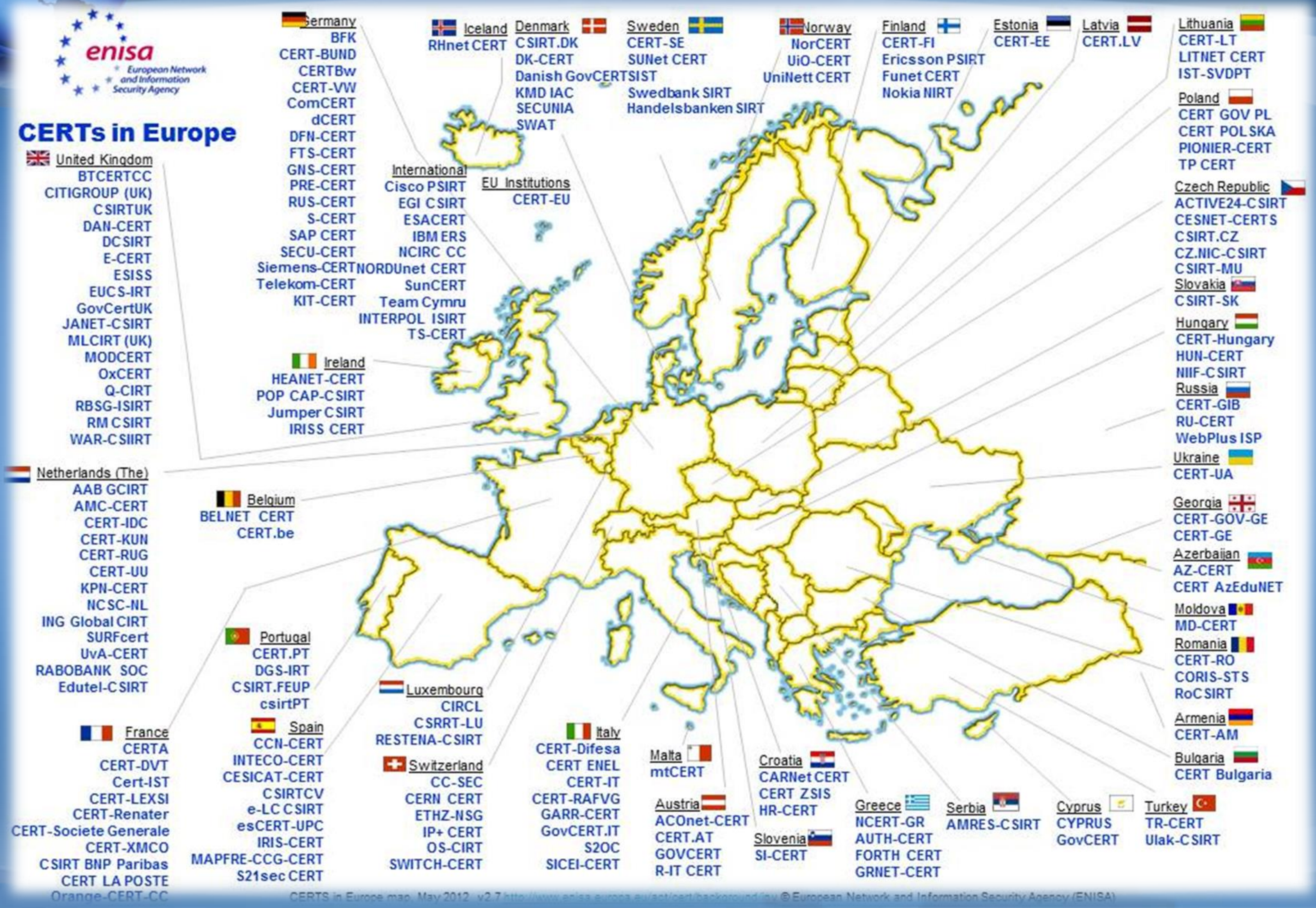
on behalf of
TERENA

Valentino Cavalli
Acting Secretary General

TERENA

TF-CSIRT Trusted Introducer
is a service of TERENA.

CERTs IN EUROPE



enisa
European Network and Information Security Agency

CERTs in Europe

United Kingdom
BTCERTCC
CITIGROUP (UK)
CSIRTUK
DAN-CERT
DCSIRT
E-CERT
ESISS
EUCS-IRT
GovCertUK
JANET-CSIRT
MLCIRT (UK)
MODCERT
OxCERT
Q-CIRT
RBSG-ISIRT
RM CSIRT
WAR-CSIIRT

Netherlands (The)
AAB GCIRT
AMC-CERT
CERT-IDC
CERT-KUN
CERT-RUG
CERT-UU
KPN-CERT
NCSC-NL
ING Global CIRT
SURFcert
UvA-CERT
RABOBANK SOC
Edutel-CSIRT

France
CERTA
CERT-DVT
Cert-IST
CERT-LEXSI
CERT-Renater
CERT-Societe Generale
CERT-XMCO
CSIRT BNP Paribas
CERT LA POSTE
Orange-CERT-CC

Germany
BFK
CERT-BUND
CERTBw
CERT-VW
ComCERT
dCERT
DFN-CERT
FTS-CERT
GNS-CERT
PRE-CERT
RUS-CERT
S-CERT
SAP CERT
SECU-CERT
Siemens-CERT
Telekom-CERT
KIT-CERT

Ireland
HEANET-CERT
POP CAP-CSIRT
Jumper CSIRT
IRISS CERT

Belgium
BELNET CERT
CERT.be

Portugal
CERT.PT
DGS-IRT
CSIRT.FEUP
csirtPT

Spain
CCN-CERT
INTECO-CERT
CESICAT-CERT
CSIRTCV
e-LC CSIRT
esCERT-UPC
IRIS-CERT
MAPFRE-CCG-CERT
S21sec CERT

International
Cisco PSIRT
EGI CSIRT
ESACERT
IBM ERS
NCIRC CC
NORDUnet CERT
SunCERT
Team Cymru
INTERPOL ISIRT
TS-CERT

EU Institutions
CERT-EU

Luxembourg
CIRCL
CSRRT-LU
RESTENA-CSIRT

Switzerland
CC-SEC
CERN CERT
ETHZ-NSG
IP+ CERT
OS-CIRT
SWITCH-CERT

Iceland
RHnet CERT

Denmark
CSIRT.DK
DK-CERT
Danish GovCERTSIST
KMD IAC
SECUNIA
SWAT

Sweden
CERT-SE
SUNet CERT
Swedbank SIRT
Handelsbanken SIRT

Norway
NorCERT
UiO-CERT
UniNett CERT

Finland
CERT-FI
Ericsson PSIRT
Funet CERT
Nokia NIRT

Estonia
CERT-EE

Latvia
CERT.LV

Italy
CERT-Difesa
CERT ENEL
CERT-IT
CERT-RAFVG
GARR-CERT
GovCERT.IT
S2OC
SICEI-CERT

Malta
mtCERT

Austria
ACOnet-CERT
CERT.AT
GOVCERT
R-IT CERT

Croatia
CARNet CERT
CERT ZSIS
HR-CERT

Slovenia
SI-CERT

Greece
NCERT-GR
AUTH-CERT
FORTH CERT
GRNET-CERT

Serbia
AMRES-CSIRT

Cyprus
CYPRUS
GovCERT

Turkey
TR-CERT
Ulak-CSIRT

Lithuania
CERT-LT
LITNET CERT
IST-SVDPT

Poland
CERT GOV PL
CERT POLSKA
PIONIER-CERT
TP CERT

Czech Republic
ACTIVE24-CSIRT
CESNET-CERTS
CSIRT.CZ
CZ.NIC-CSIRT
CSIRT-MU

Slovakia
CSIRT-SK

Hungary
CERT-Hungary
HUN-CERT
NIIF-CSIRT

Russia
CERT-GIB
RU-CERT
WebPlus ISP

Ukraine
CERT-UA

Georgia
CERT-GOV-GE
CERT-GE

Azerbaijan
AZ-CERT
CERT AzEduNET

Moldova
MD-CERT

Romania
CERT-RO
CORIS-STS
RoCSIRT

Armenia
CERT-AM

Bulgaria
CERT Bulgaria

CERTS in Europe map, May 2012, v2.7 http://www.enisa.europa.eu/act/cert/background/inv © European Network and Information Security Agency (ENISA)

MISSION OF GOVCERT BG

Assist users in performing proactive activities aimed at reducing the risks in incidents in information security and assist in handling such incidents when occurred.

SERVICES PROVIDED BY CERT BG AT THE MOMENT

Alerts and Warnings

Vulnerability Handling

Incident Handling

Artifact Handling

Announcements

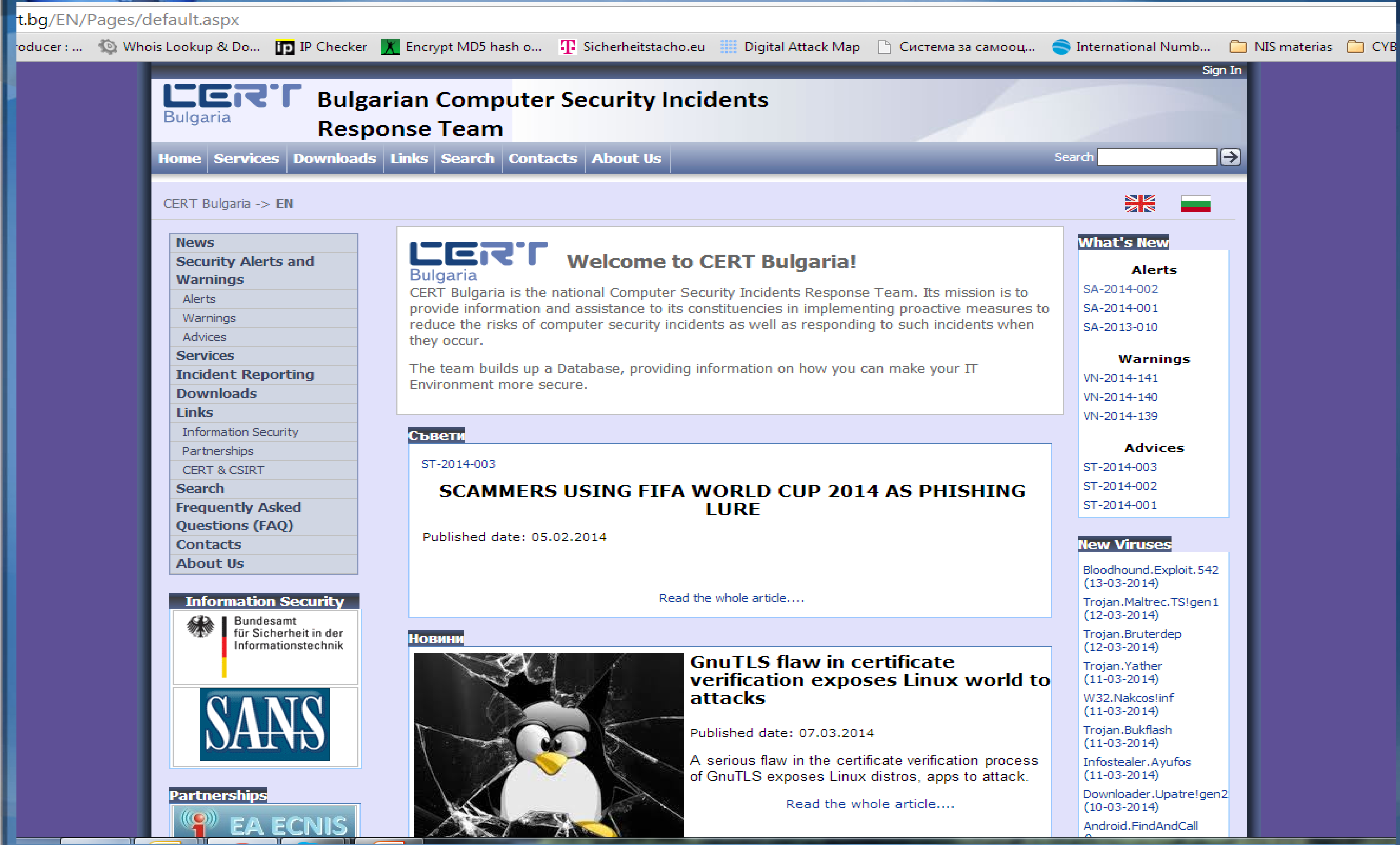
Security-Related Information Dissemination

OBJECTIVES OF CERT BG

- Protection of information and technological assets;
- Reducing the impact of security incidents on the information society;
- Providing assistance in recovering from incidents;
- Evaluating the influence of incidents on the security of systems;
- Disseminating technical information related to computer security incidents;
- Conducting studies related to new network and information security technologies;
- Organizing education and awareness raising related to information security.

Executive Agency “Electronic Communication Networks and Information Systems”, MTITC

HTTPS://GOVCERT.BG



t.bg/EN/Pages/default.aspx

CERT Bulgaria

Bulgarian Computer Security Incidents Response Team

CERT Bulgaria -> EN

CERT Bulgaria

Welcome to CERT Bulgaria!

CERT Bulgaria is the national Computer Security Incidents Response Team. Its mission is to provide information and assistance to its constituencies in implementing proactive measures to reduce the risks of computer security incidents as well as responding to such incidents when they occur.

The team builds up a Database, providing information on how you can make your IT Environment more secure.

Съвети

ST-2014-003

SCAMMERS USING FIFA WORLD CUP 2014 AS PHISHING LURE

Published date: 05.02.2014

Read the whole article....

Новини

GnuTLS flaw in certificate verification exposes Linux world to attacks

Published date: 07.03.2014

A serious flaw in the certificate verification process of GnuTLS exposes Linux distros, apps to attack.

Read the whole article....

What's New

Alerts

SA-2014-002
SA-2014-001
SA-2013-010

Warnings

VN-2014-141
VN-2014-140
VN-2014-139

Advices

ST-2014-003
ST-2014-002
ST-2014-001

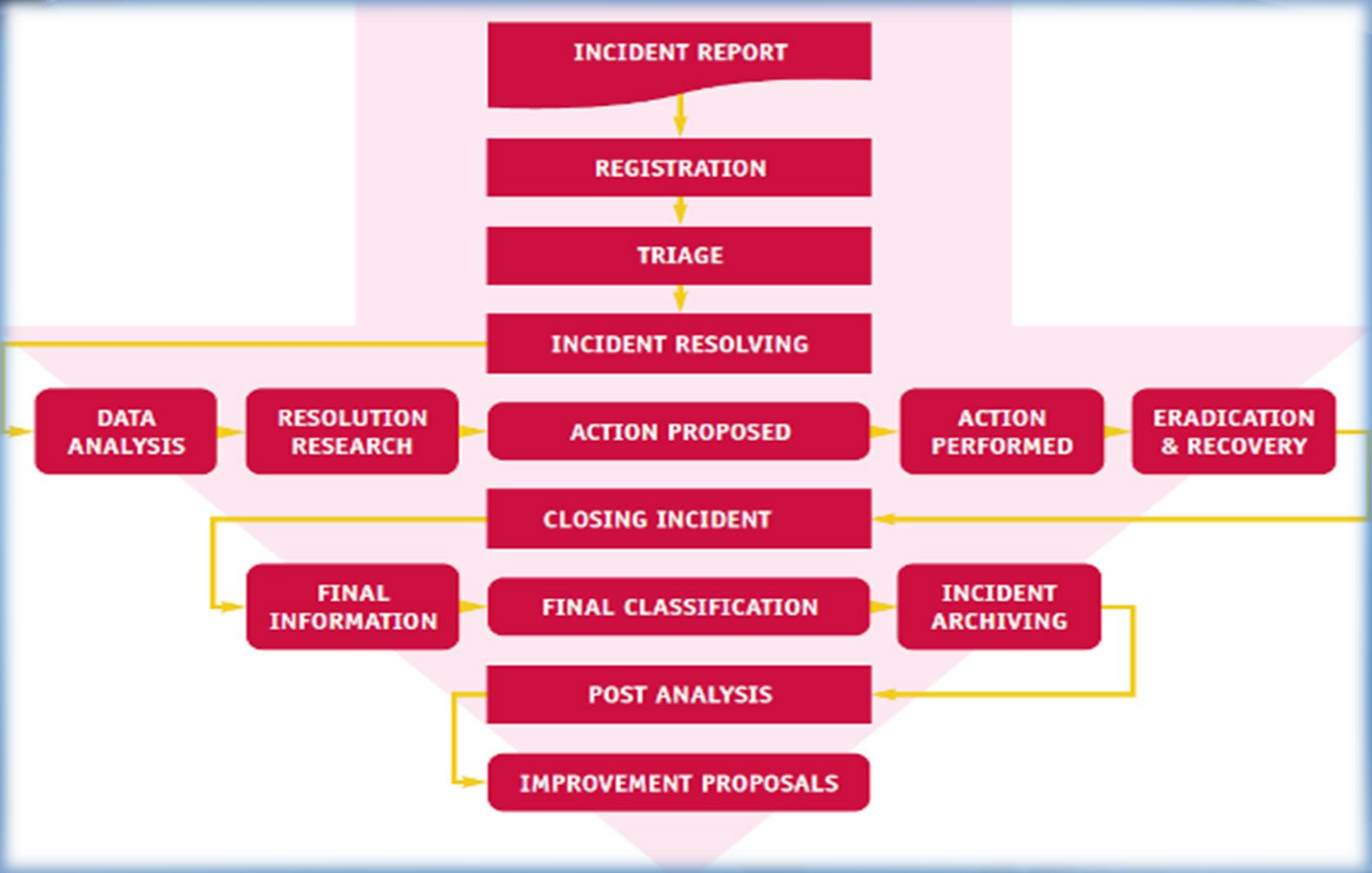
New Viruses

Bloodhound.Exploit.542 (13-03-2014)
Trojan.Maltrec.TS!gen1 (12-03-2014)
Trojan.Bruterdep (12-03-2014)
Trojan.Yather (11-03-2014)
W32.Nakcos!inf (11-03-2014)
Trojan.Bukflash (11-03-2014)
Infostealer.Ayufos (11-03-2014)
Downloader.Upatre!gen2 (10-03-2014)
Android.FindAndCall

E-mail

C@LL

INCIDENT HANDLING WORKFLOW



COMMON LANGUAGE SECURITY INCIDENT TAXONOMY

INCIDENT						
	ATTACK(S)					
			EVENT			
Attackers	Tool	Vulnerability	Action	Target	Unauthorized Results	Objectives
Hackers	Physical Attack	Design	Probe	Account	Increased Access	Challenge Status, Thrill
Spies	Information Exchange	Implementation	Scan	Process	Disclosure of Information	Political Gain
Terrorists	User Command	Configuration	Flood	Data	Corruption of Information	Financial Gain
Corporate Raiders	Script or Program		Authenticate	Component	Denial of Service	Damage
Professional Criminals	Autonomous Agent		Bypass Spoof	Computer	Theft of Resources	
Vandals	Toolkit		Read	Network		
Voyeurs	Distributed Tool		Copy	Internetwork		
	Data Tap		Steal			
			Modify			
			Delete			

FULL CLASSIFICATION SCHEMA OF ENISA TAXONOMY

Abusive Content

- Spam;
- Harassment;
- Child/Sexual/Violence/...

Malicious Code

- Virus;
- Worm;
- Trojan;
- Spyware;
- Dialler.

Information Gathering

- Scanning;
- Sniffing;
- Social Engineering;

Intrusion Attempts

- Exploiting known;
- Vulnerabilities;
- Login Attempts;
- New Attack Signature;

Intrusions

- Privileged Account Compromise;
- Unprivileged Account Compromise;
- Application Compromise;
- Botnet.

Availability

- DoS;
- DDoS;
- Sabotage;

Information Security

- Unauthorised access to information;
- Unauthorised modification of information;

Fraud

- Unauthorised use of resources;
- Copyright;
- Masquerade;
- Phishing.

OTHER …

COOPERATION

TI TF-CSIRT Trusted Introducer

enisa European Network and Information Security Agency

CERT

EGC group

FIRST Improving Security Together

TERENA

CERT HUNGARY

US-CERT

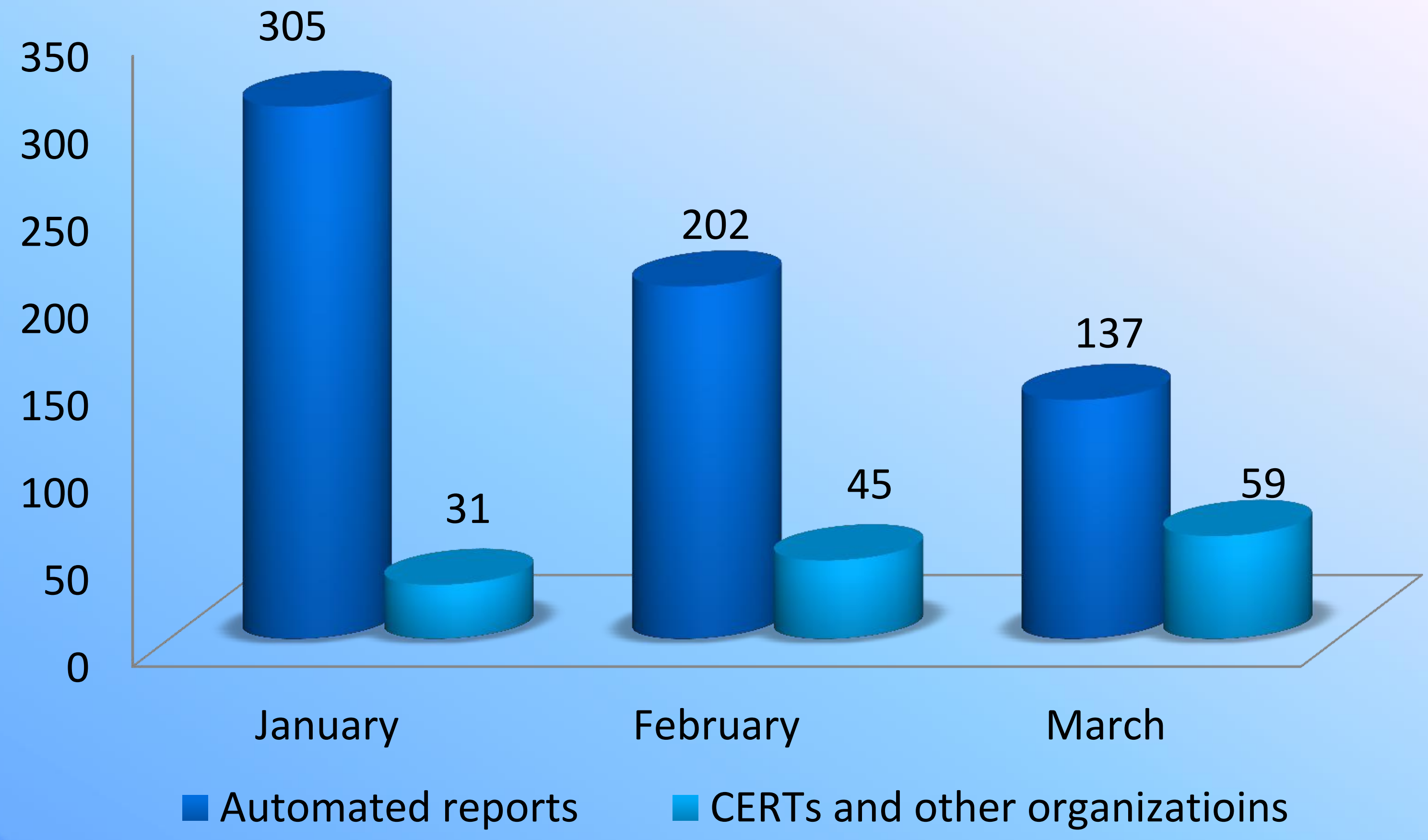
ITU International Telecommunication Union

NATO OTAN

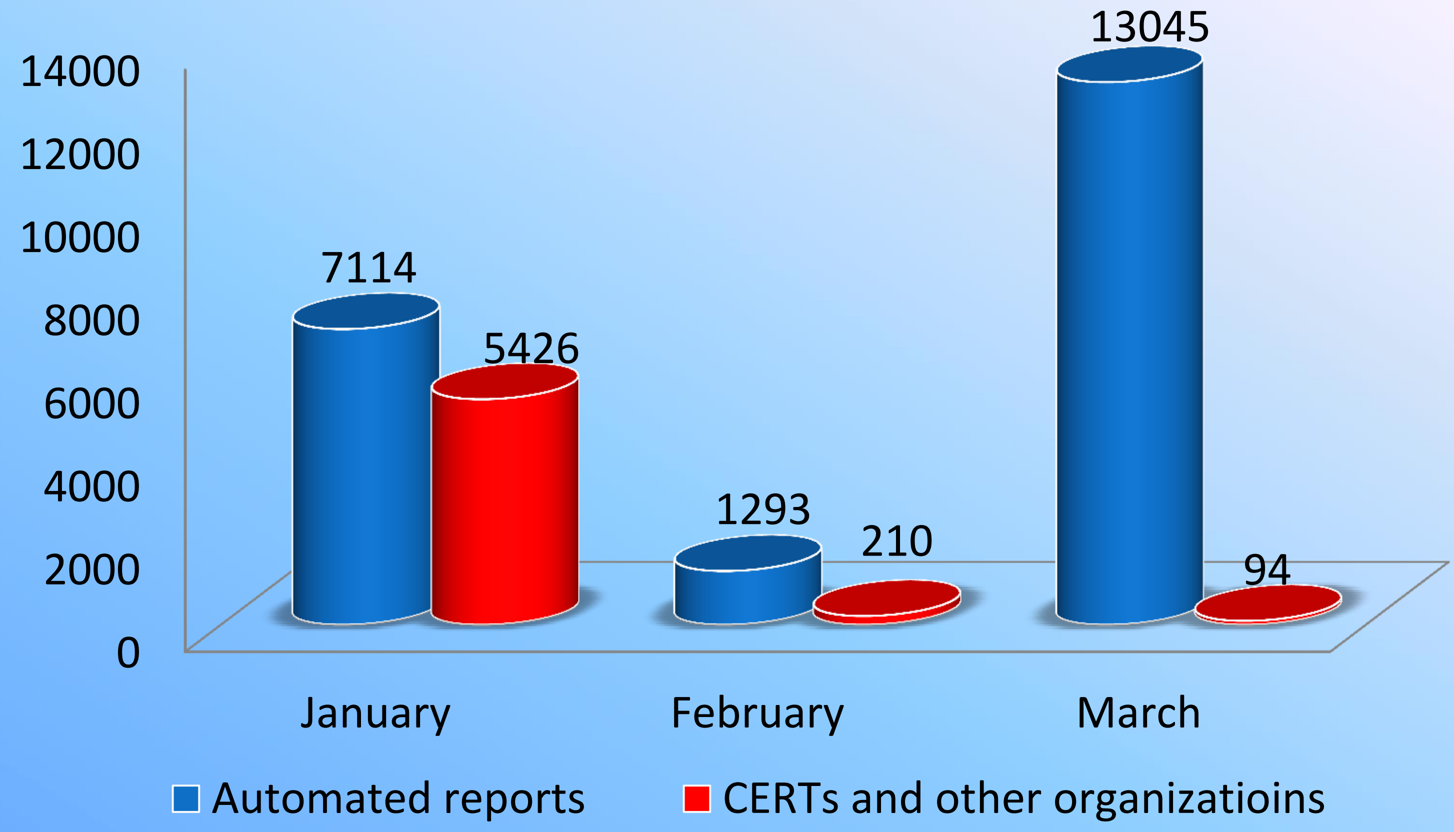
IMPACT

INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

INCIDENTS REPORT

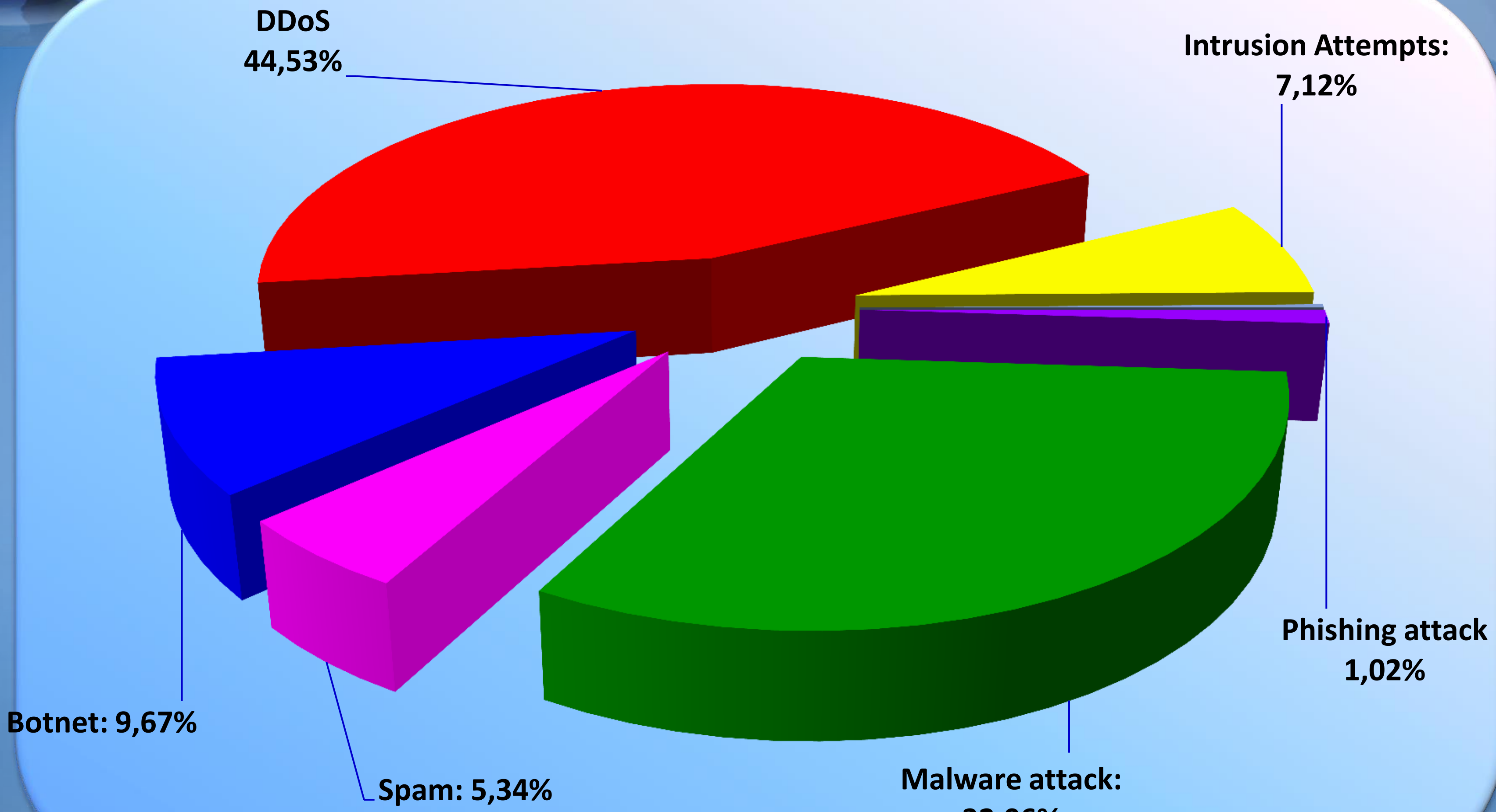


NUMBER OF IP ADDRESSES INVOLVED

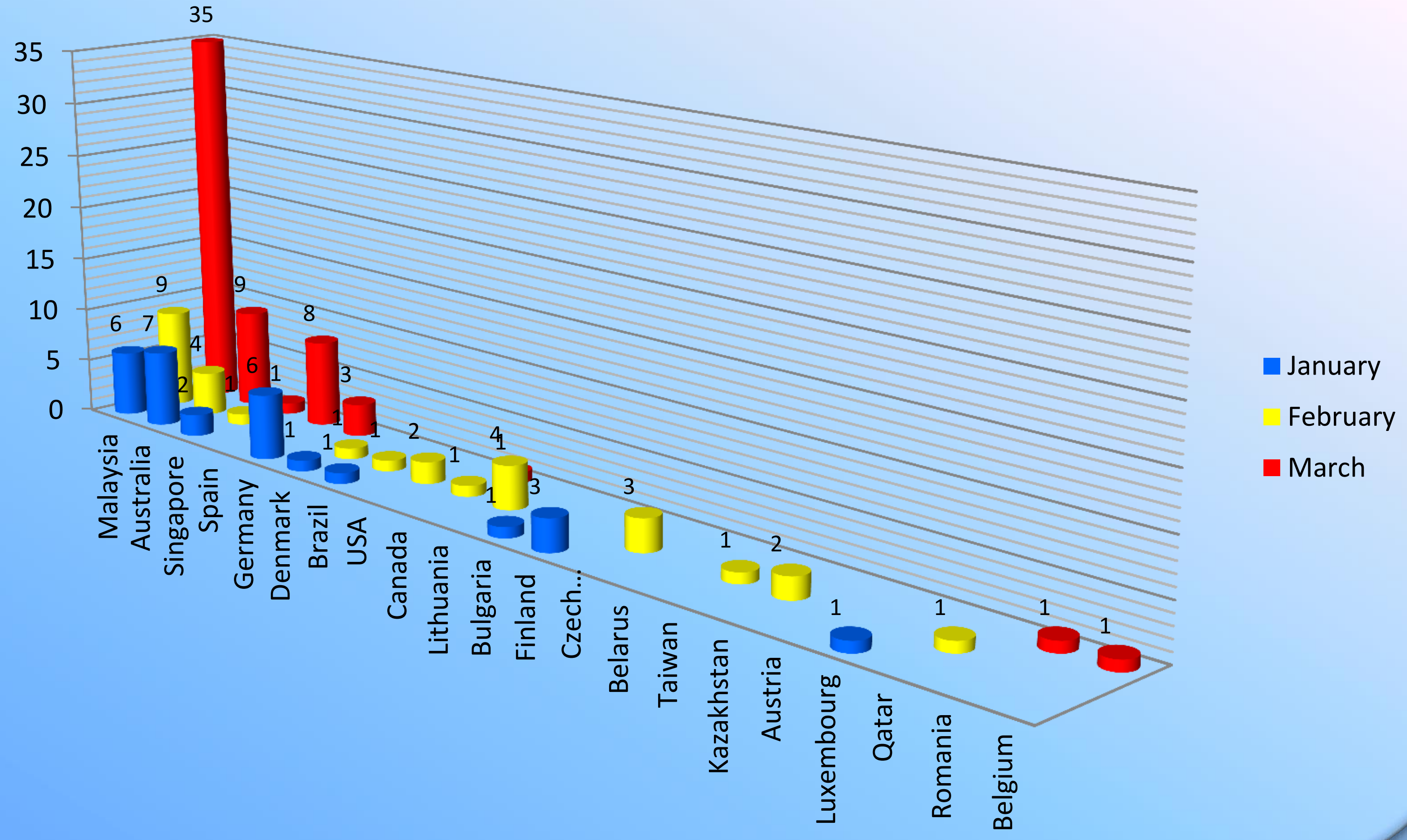


Executive Agency “Electronic Communication Networks and Information Systems”, MTITC

TYPES OF CYBER ATTACKS



NUMBER OF SIGNALS REPORTED BY COUNTRIES



THANK YOU!