Session II: the criminal justice response

The tools of the Convention on Cybercrime

Alexander Seger

Head of Cybercrime Division

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

EUROJUST

The problem of cybercrime …

Cybercrime To Cost The World $10.5 Trillion Annually By 2025

Every U.S. business is under cyberattack

Email | Print Friendly | Share

November 18, 2020 11:03 ET | **Source:** INTRUSION Inc.

PLANO, Texas, Nov. 18, 2020 (GLOBE NEWSWIRE) -- **Cybersecurity Ventures** predicts global cybercrime costs will grow by 15 percent per year over the next five years, reaching **$10.5 trillion USD annually by 2025**, up from $3 trillion USD in 2015. This prediction is part of a

Profile
INTRUSION In

Subscribe

SECURITY

IBM finds phishing threat to covid-19 vaccine 'cold chain'

…ion efforts... without the right …
…sn't stand a chance.

Home » Security Bloggers Network » 40% Increase in Ransomware Attacks in Q3 2020

40% Increase in Ransomware Attacks in Q3 2020

by saptarshi das on November 16, 2020

The Week in Ransomware - November 27th 2020 - Attacks continue

By Lawrence Abrams

Artificial intelligence could be used to hack connected cars, drones warn security experts

Cyberattacks on vulnerabilities in connected vehicles could have very real physical consequences if security isn't managed properly.

By Danny Palmer | November 20, 2020 -- 12:40 GMT (12:40 GMT) | Topic: Security

CYBER BULLYING

MORE FROM

DNA Exclusive: Women soft target of cyberbullying online violence on social media

In a shocking report, about 35 per cent of the women in the world are victims of some or the other kind of cyber violence. The DNA analysis will look into the different aspects of cyber violence against women relate… to nearly 400 million women around the world.

Comment les acteurs du cybercrime se professionnalisent

Par Sophy Caulier

Publié le 15 novembre 2020 à 18h00 - Mis à jour le 16 novembre 2020 à 11h59

Réservé à nos abonnés

Partage

ENQUÊTE | **En plein essor, très lucrative, la criminalité sur Inter… est passée de la petite délinquance au crime organisé. L'agili…**

Warning: Domestic cyber terrorism on the rise in 2021

SPECIAL

BY TIM SANDLE NOV 25, 2020 IN BUSINESS

LISTEN | PRIN…

This year has been rocky, yet as businesses attempt to re-build for 2021, next year will see a continuation of challenges and some new threats emerging. These … external to the nation state.

Costa Rica's 'War' Against Ransomware Is a Wake-Up Call for the Region

James Bosworth

Jul 18, 2022

News, World

Covid-19 lockdowns drive spike in online child abuse

Published December 3, 2020, 6:39 AM
by Agence France-Presse

Post Covid, corporates …

…st Updated: Dec 02, 2020, 05:00 PM IST

US issues rare security alert as Montenegro battles ongoing ransomware attack

Manchester United …

previous calendar m…

… and e-evidence re all types of crime

Cybercrime To Cost The World $10.5 Trillion Annually B

Every U.S. busines

November 18, 2020 11:03 ET | Source: INTRUSION Inc.

PLANO, Texas, Nov. 18, 2020 (GLOBE NEWSWIRE) -- Cybersecurity Ventures predicts global cybercrime costs will grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This prediction is part of a

nds phishing

threat to covid-19

vaccine 'cold

The V vare - November 27th 2020 - Attacks continue

By Lawrence Abrams

Comment les acteurs du cy

prof

Par Sophy Caulier

Publié le 15 novembre 2020 à 18h00 - Mis à jo

Réservé à nos abonnés

Partage

Artificial intelligence could be use

connected cars, drones warn secu

Cyberattacks on vulnerabilities in connected vehicles could have very real physical consequ

managed properly.

By Danny Palmer | Novem 20, 2020 -- 12:40 GMT (12:40 GMT) |

Topic: Security

Warning: Domestic cyber terrorism on the

2021 SPECIAL

BY TIM SANDLE NOV 25, 2020 IN BUSINESS

LISTEN | PRINT

vet as businesses attempt to re-build for 2021 next year

me new threats emerging. These

d external to the nation state.

ENQUÊTE | En plein essor, très lucrative, la criminalité sur Int

est passée de la petite délinquance au crime organisé. L'ac

News, World

Covid-19 lockdowns drive spike in online child abuse

Published December 3, 2020, 6:39 AM

by Agence France-Presse

Post Covid, corporates see huge increase in cyber crimes

IST

Home » Security Bloggers Network » 40% Increase in Ransomware Attacks

40% Increase in Ransomware Atta

by saptarshi das on November 16, 2020

MORE FROM DANNY PA

CYBERBULLYING

DNA Exclusive: Women soft target of cyberbullying, online violence on social media

In a shocking report, about 35 per cent of the women in the world are victims of some or the other kind of cyber violence. The DNA analysis will look into the different aspects related to nearly 400 million women around the world.

A roundup of UK focused Cyber and Information Security News, Blog Posts, Reports and general Threat Intelligence from the previous calendar month, November 2020.

cyber-attack, which I covered in a blog post titled The Multi-Millio

provided few details about their cyber-attack which has been

dia are widely reporting United's leaky IT defences was

kney Borough Council have also been tight-lipped abou

pacted its service delivery to Londoners. Like United, this attack

Evidence on a computer system

Online sexual violence against children

COVID-19 related crime

WARCRIME

Violence against women

Election interference

ANY CRIME

Terrorism

Medicrime

Money laundering

Hate crime

Financial crime

Kidnapping

Corruption

Murder

Fraud

The mechanism of the Convention on Cybercrime

Budapest Convention on Cybercrime (2001):

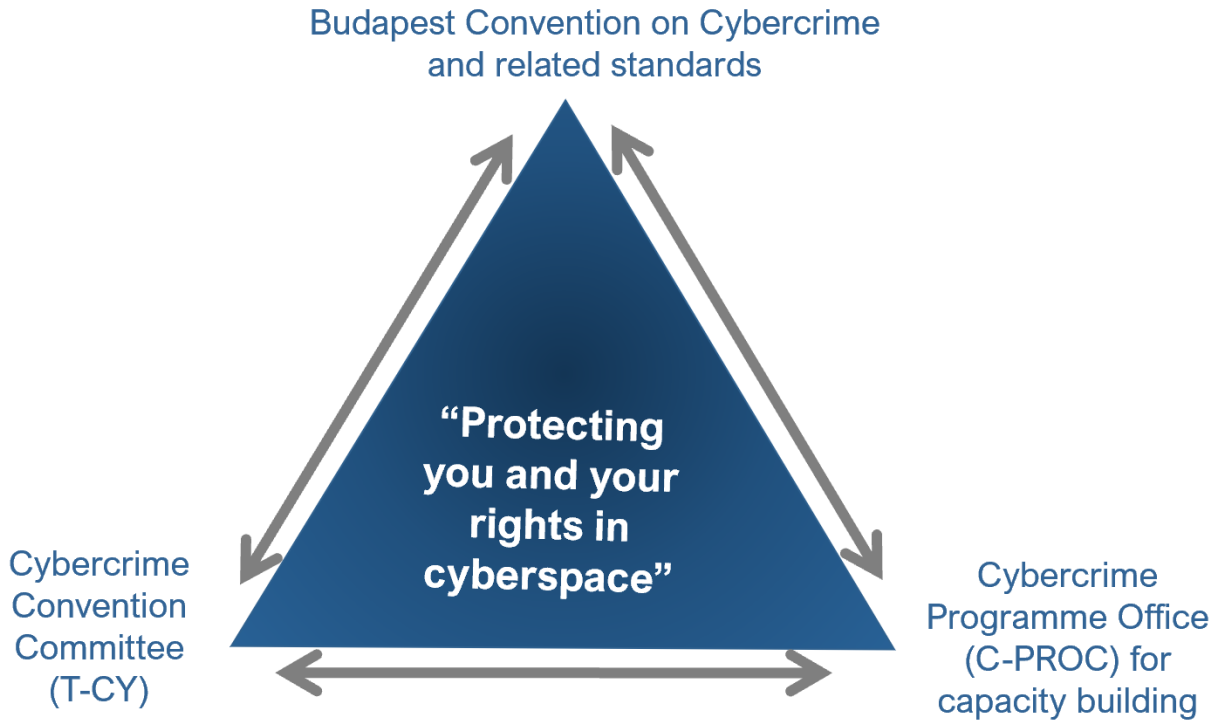
1. Specific offences against and by means of computer systems
2. Procedural powers with safeguards to investigate cybercrime and collect electronic evidence in relation to any crime
3. International cooperation on cybercrime and e-evidence

+ 1st Protocol on Xenophobia and Racism via Computer Systems

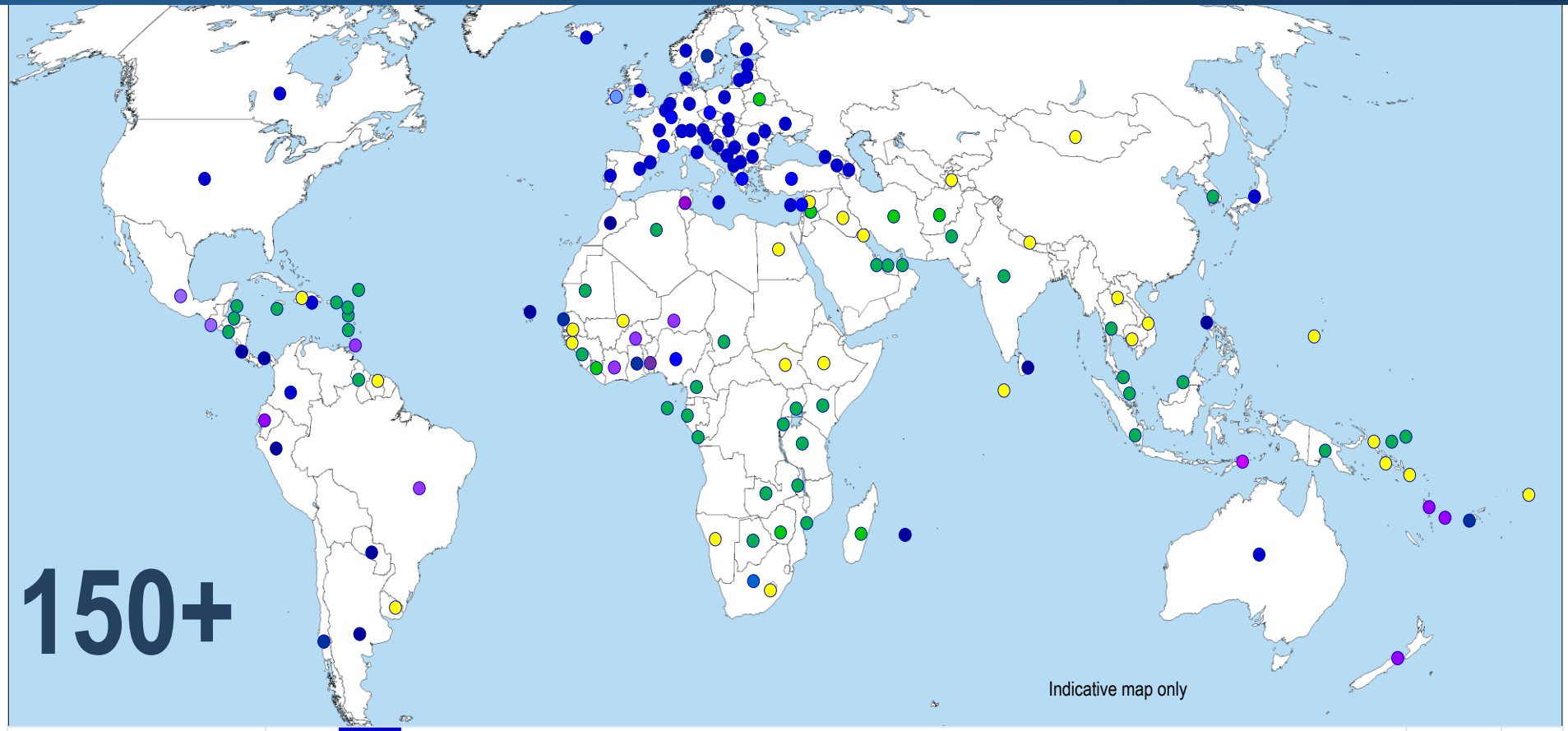
+ Guidance Notes

+ 2nd Protocol on enhanced cooperation on cybercrime and electronic evidence (opened for signature 12 May 2022)

By October 2022: **67 Parties and 16 Observer States**



Reach of the Convention on Cybercrime



Parties:	67				
Signed:	2		Other States with substantive laws broadly in line with Budapest Convention:	45+	
Invited to accede:	14		Further States drawing on Budapest Convention for legislation:	30+	
=	**83**		=	**75+**	

The Convention on Cybercrime: Backed up by capacity building

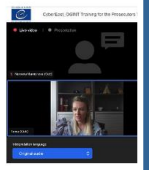
Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania:

- Support processes of change towards stronger criminal justice capacities on cybercrime and e-evidence in line with the Budapest Convention and with rule of law safeguards
- 5 ongoing projects with a cumulative budget of EUR 38+ million
- 38 staff
- Some 400 activities per year
- Capacity for virtual capacity building
- Cooperation with 120+ countries in 2021/2022
- Joint projects with the European Union
- Voluntary contributions by Canada, Hungary, Italy, Japan, UK and USA in 2021/2
- Support to T-CY

Current projects:

- GLACY+
- CyberEast
- CyberSouth
- iPROCEEDS-2
- Octopus

Workshop or



detectives of
male) increas

This is the re

Union, held a
cybercrime and electronic evidence with the provisions of the Budapest Convention on...

CyberSouth: Workshop on cybercrime legislation in Jordan

ing national delivery of an introductory course
d electronic evidence in Benin

)U, BENIN

ember, a group of judges and prosecutors from Benin, who had
ted workshop earlier in August, delivered for the first time an
:e to their peers. During the first...

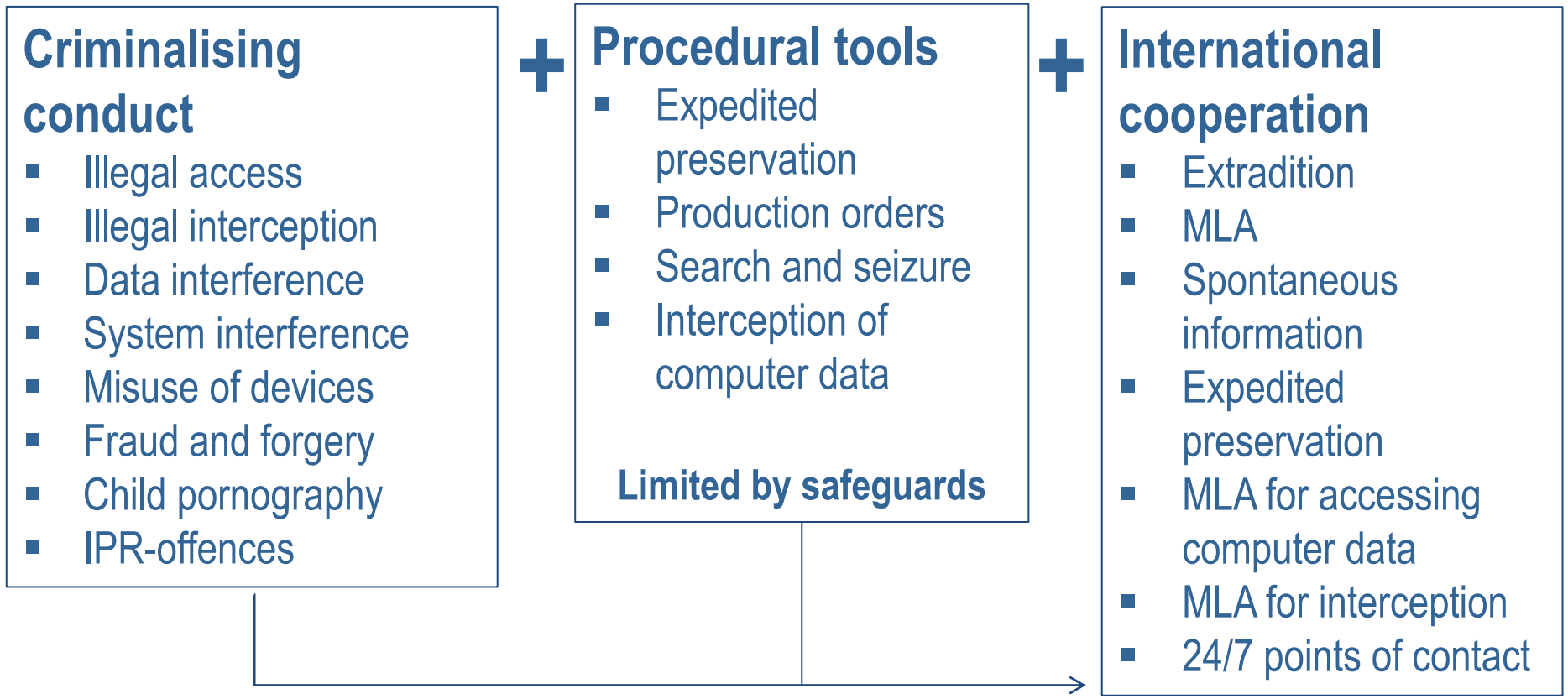
)nom
)pera
SBOURG,
)22, the
)pe. This
)ught to
co-
:POL:
's of t
E AND CA
evidenc
erde, Ga
arge
e of

\CY+: 9th Africa Working Group on
in Rwanda

IDA

g partner of the GLACY+ Project, organised the 9th Africa Working
in Rwanda from 18 to 22 July 2022. The AF-WGM is an annual
t practices in the region. This...

Content of the Budapest Convention



Procedural powers and international cooperation for any criminal offence involving evidence on a computer system!

Challenges

Cybercrime: Threat to

- Human rights
- Democracy
- Rule of law

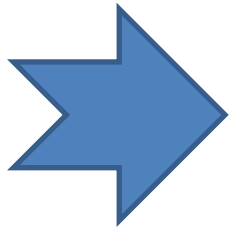
Positive obligations:

- Provide the means to protect the rights of individuals, also against crime

Problem:

- Proliferation of cybercrime
- Any type of crime now involving e-evidence
- Evidence somewhere in foreign, multiple, shifting or unknown jurisdictions
- Effective means not available to obtain the disclosure of e-evidence

- Less than 0.1% of offences in cyberspace lead to prosecutions and convictions
- Do victims obtain justice?



2nd Protocol to help address these challenges

2nd Additional Protocol to the Convention on Cybercrime: content

Preamble

Chapter I: Common provisions

- Article 1 Purpose
- Article 2 Scope of application
- Article 3 Definitions
- Article 4 Language

Chapter II: Measures for enhanced cooperation

- Article 5 General principles applicable to Chapter II
- Article 6 Request for domain name registration information
- Article 7 Disclosure of subscriber information
- Article 8 Giving effect to orders from another party for expedited production of subscriber information and traffic data
- Article 9 Expedited disclosure of stored computer data in an emergency
- Article 10 Emergency mutual assistance
- Article 11 Video conferencing
- Article 12 Joint investigation teams and joint investigations

Chapter III – Conditions and safeguards

- Article 13 Conditions and safeguards
- Article 14 Protection of personal data

Chapter IV: Final provisions

- Article 15 Effects of this Protocol
- Article 16 Signature and entry into force
- Article 17 Federal clause
- Article 18 Territorial application
- Article 19 Reservations and declarations
- Article 20 Status and withdrawal of reservations
- Article 21 Amendments
- Article 22 Settlement of disputes
- Article 23 Consultations of the Parties and assessment of implementation
- Article 24 Denunciation
- Article 25 Notification

2nd Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (CETS 224)

Signatories (status 2 Nov 2022):

1. Andorra
2. Austria
3. Belgium
4. Bulgaria
5. Chile
6. Colombia
7. Costa Rica
8. Estonia
9. Finland
10. Iceland
11. Italy
12. Japan
13. Lithuania
14. Luxembourg
15. Montenegro
16. Morocco
17. Netherlands
18. North Macedonia
19. Portugal
20. Romania
21. Serbia
22. Spain
23. Sweden
24. USA

Next:

- ► Signature by other Parties
- ► Ratification (5 needed for entry into force)
- ► Capacity building

Does the Convention (with Protocols) cover ransomware-related offences?

future tense

How the Worst Cyberattack in History Hit American Hospitals

NotPetya caused $10 billion in damage. But it may have also taken a toll on patients' health across the U.S.

BY ANDY GREENBERG NOV 05, 2019 • 5:40 AM

UK suffers third highest number of ransomware attacks globally

Based on an analysis of around 5,000 ransomware incidents, NordLocker has found that UK businesses, and small businesses in particular, are a priority target for ransomware gangs

By Sebastian Klovig Skelton, Senior reporter Published: 28 Sep 2022 13:45

US issues rare security alert as Montenegro battles ongoing ransomware attack

Carly Page @carlypage_ / 3:42 PM GMT+2 • August 31, 2022 Comment

Posted 1:06PM on Thursday 12th May 2022 (4 months ago)

Costa Rica declares emergency in ongoing cyber attack

SHARE TWEET

By The Associated Press

Contact Editor

SAN JOSE, Costa Rica (AP) — After a month of crippling ransomware attacks, Costa Rica has declared a state of emergency. In theory, the measure usually reserved to deal with natural disasters or the COVID-19 pandemic would free

The Costa Rica Ransomware Attacks: The Implications of Cyberattacks on Critical Infrastructure

Posted on August 11, 2022 by JP Perez-Etchegoyen in Best Practices

WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017

Most first encountered ransomware after an outbreak shut down hospital computers and diverted ambulances this year. Is it here to stay?

Costa Rica's 'War' Against Ransomware Is a Wake-Up Call for the Region

James Bosworth Jul 18, 2022

Content of the Budapest Convention: example ransomware

Article	Budapest Convention on Cybercrime
Art. 2	Illegal access
Art. 3	Illegal interception
Art. 4	Data interference
Art. 5	System interference
Art. 6	Misuse of devices
Art. 7	Computer-related forgery
Art. 8	Computer-related fraud
Art. 11	Attempt, aiding, abetting
Art. 12	Corporate liability
Art. 13	Sanctions and measures

Article	Convention on Cybercrime
Art. 14-21	Procedural powers

Article	Convention on Cybercrime
Art. 23-35	International cooperation

Article	2nd Additional Protocol to Convention on Cybercrime
Art. 7	(Direct) Disclosure of subscriber information
Art. 8	Giving effect to orders from another party for expedited production of subscriber information and traffic data
Art. 9	Expedited disclosure of stored computer data in an emergency
Art. 10	Emergency mutual assistance
Art. 11	Video conferencing
Art. 12	Joint investigation teams and joint investigations

Conclusion

- The tools are there.
- Become a Party to the Budapest Convention on Cybercrime
- Sign, implement and ratify the Second Additional Protocol
- Engage in capacity building