



# GLACY+

Global Action on Cybercrime Extended  
Action Globale sur la Cybercriminalité Élargie

Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe

## **EU/COE Joint Project on Global Action on Cybercrime**

# **Legislation on cybercrime: Substantive criminal law**

**Joint ECOWAS-Council of Europe regional conference**

**Mutual Assistance Requests: Procedures for requesting electronic  
evidence from international partners**

**Abuja, Nigeria – 11 September 2017**

**Zahid Jamil**

Council of Europe Expert, Pakistan

# The approach of Council of Europe

## 1 Common standards: Budapest Convention on Cybercrime and related standards

2 Follow up and assessments:  
Cybercrime  
Convention  
Committee (T-CY)



3 Capacity  
building:  
C-PROC ►  
Technical  
cooperation  
programmes



# Budapest Convention: scope

## **Criminalising conduct**

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

## **Procedural tools**

- Expedited preservation
- Partial disclosure of traffic data
- Production orders
- Search and seizure
- Interception of computer data

+

## **International cooperation**

- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

**Harmonisation**



# International Cooperation

# Informal Cooperation

- Discretionary
- Faster when works
- Seldom work
- Not evidence
- Usually uneven playing field
- Usually refusals



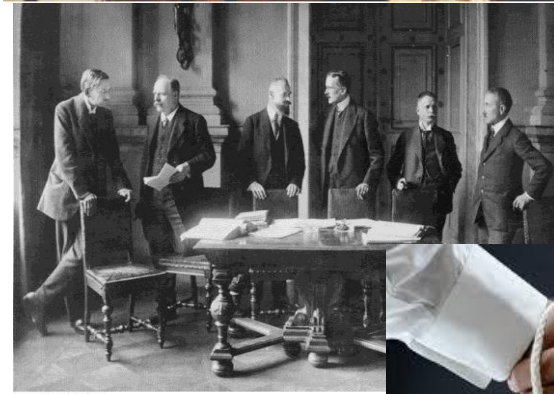
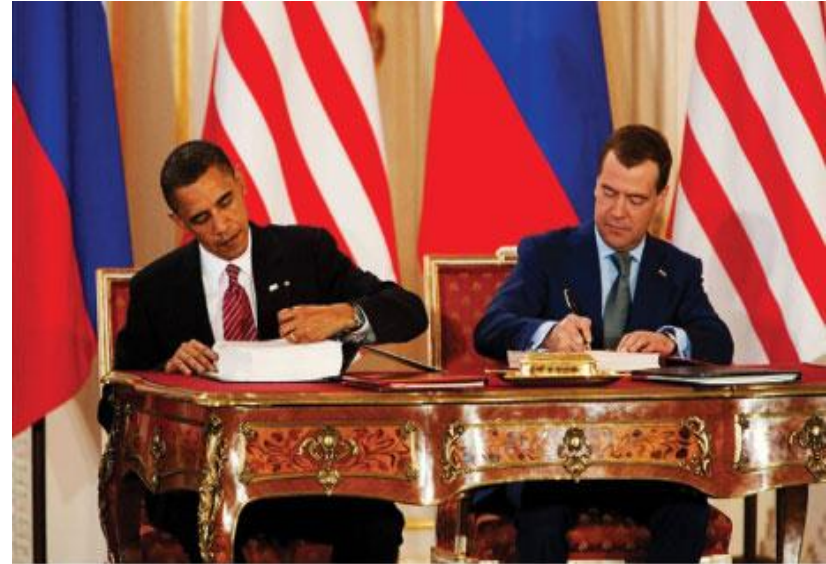
Examples:





# Formal Cooperation: Treaty or Convention

- Bilateral MLATs
- Archaic provisions
- Slow
- Not always lead to cooperation
- Every country
- Not a cyber solution
- Need modernization
- One country at a time
- Regional - geographic limitations







# Examples:





# NEED:

Formal International obligation

Catches up with the speed of  
informal process

Human rights

Confidence & Trust

Limited to criminal justice



- Harmonize laws
- Not technologically specific or else become archaic
- Not have everything or else no consensus.
- Baseline. Inclusive treaty.
- Harmonize procedures
- Harmonized cross border procedures and cooperation
- Not mutually exclusive. Complimentary
- Members include those where data held and cooperation sought



## Majority of Request Flows:

# Infrastructure States to Developing States



# **Case Study: Avalanche Network**



Consider this situation:

**600 servers  
globally**

**1,000,000  
emails per day  
with malware**

**BOTNET**

**800,000  
Domains used**

**Victims in  
180 countries**

**500,000  
infected  
devices**



Consider this situation:

**Phishing**

**Moneymule  
schemes**

**17 different  
Malware types**

**BOTNET**

**Banking  
Trojans**

**Malware  
campaigns**

**DDoS Attacks**





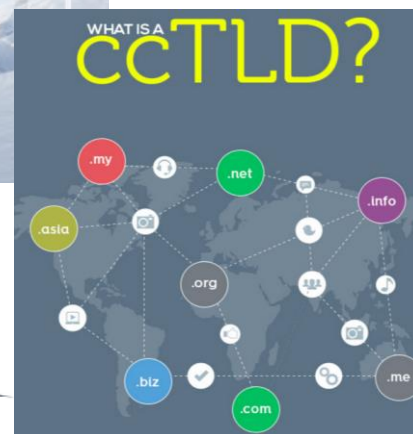
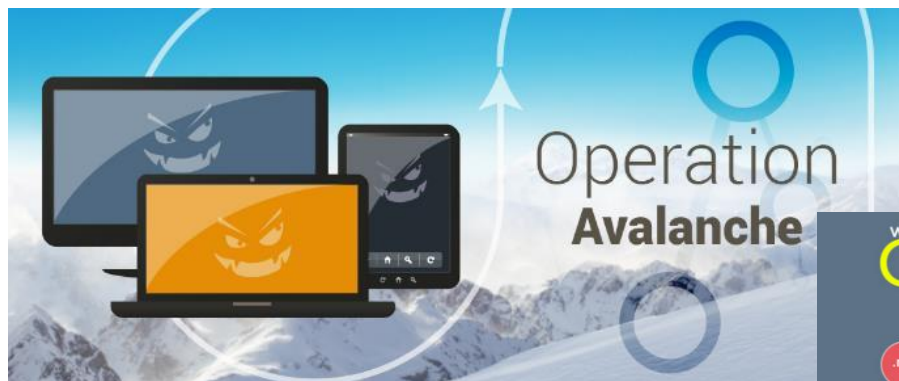
Could you cope?

## **Avalanche Crime Network**

- ❖ Started with a Ransomware attack in Germany
- ❖ Four year investigation by German Police
- ❖ 30 November 2016 swoop
- ❖ 30 countries involved with FBI, Europol, Interpol
- ❖ 37 premises searched
- ❖ 39 servers seized, 221 servers put off-line

How many arrests? 20? 50? 100?

**Just 5 arrests**



**RoLR**





## 30 countries - Prosecutors & Investigators

### 5 arrested

37 premises searched

### 39 servers seized

Over 180 countries Victims of malware identified

### 221 servers offline

(abuse notifications to hosting providers)

### Over 800 000 domains seized, sinkholed or blocked

Largest-ever use of sinkholing to combat botnet infrastructures  
unprecedented in scale

## FIGURES AT A GLANCE

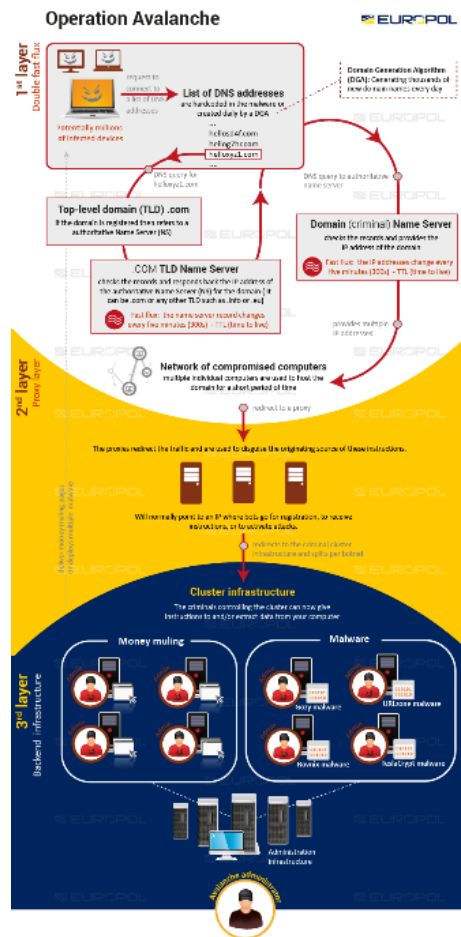
**Countries involved:** Armenia, Australia, Austria, Azerbaijan, Belgium, Belize, Bulgaria, Canada, Colombia, Finland, France, Germany, Gibraltar, Hungary, India, Italy, Lithuania, Luxembourg, Moldova, Montenegro, Netherlands, Norway, Poland, Romania, Singapore, Sweden, Taiwan, Ukraine, United Kingdom and United States of America.

Arrests: 5

Searches conducted: 37

Servers seized: 39

Servers taken offline through abuse notifications: 221



# Operation Avalanche



1st layer  
Double fast flux

Potentially millions of infected devices connected to the internet request to connect to a list of addresses



Computers connected to the Internet use name servers to resolve human readable domain names into the IP addresses used to route the IP network traffic (e.g. [www.europol.europa.eu](http://www.europol.europa.eu) has the following IP: 158.169.131.22). Usually one domain is delegated to one IP address for a long period of time.

A Domain Generation Algorithm (DGA) generates thousands of new domain names every day

hellosd4f.com, hellog7hr.com, helloxy1.com, ....

request to connect

## Name Server

is used to resolve the domain name



**Fast Flux:** the name server record changes every five minutes (300s) - TTL (time to live)

The Avalanche platform uses a complex system of **Double Fast Flux** networks and layers of proxy servers to rapidly change the apparent location of IP address records from a domain and the name servers that resolve it, with the aim of making it more difficult for Law Enforcement to trace and take down hosted criminal infrastructures.

The technique known as Fast Flux involves automatically and frequently changing the IP address records associated with a domain name. Single Fast Flux changes the IP address used to host address records associated with a domain (such as a website name). **Double Fast Flux** changes both the IP address records and the name server that is used to resolve the domain too.

## IP Address Record

provides the IP address of the domain



**Fast Flux:** the IP addresses change every five minutes (300s) - TTL (time to live)

2nd layer  
Proxy layer

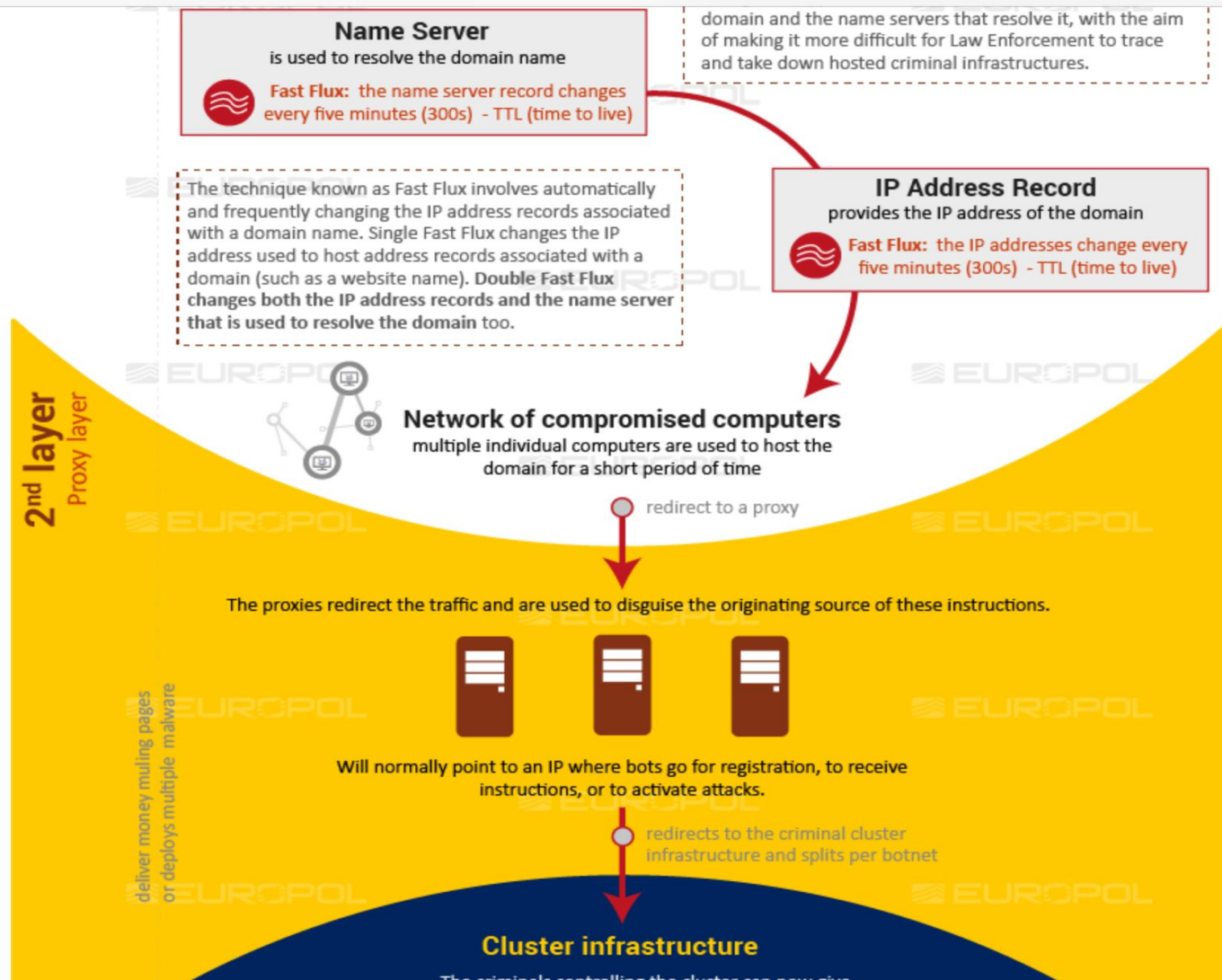


## Network of compromised computers

multiple individual computers are used to host the domain for a short period of time



redirect to a proxy





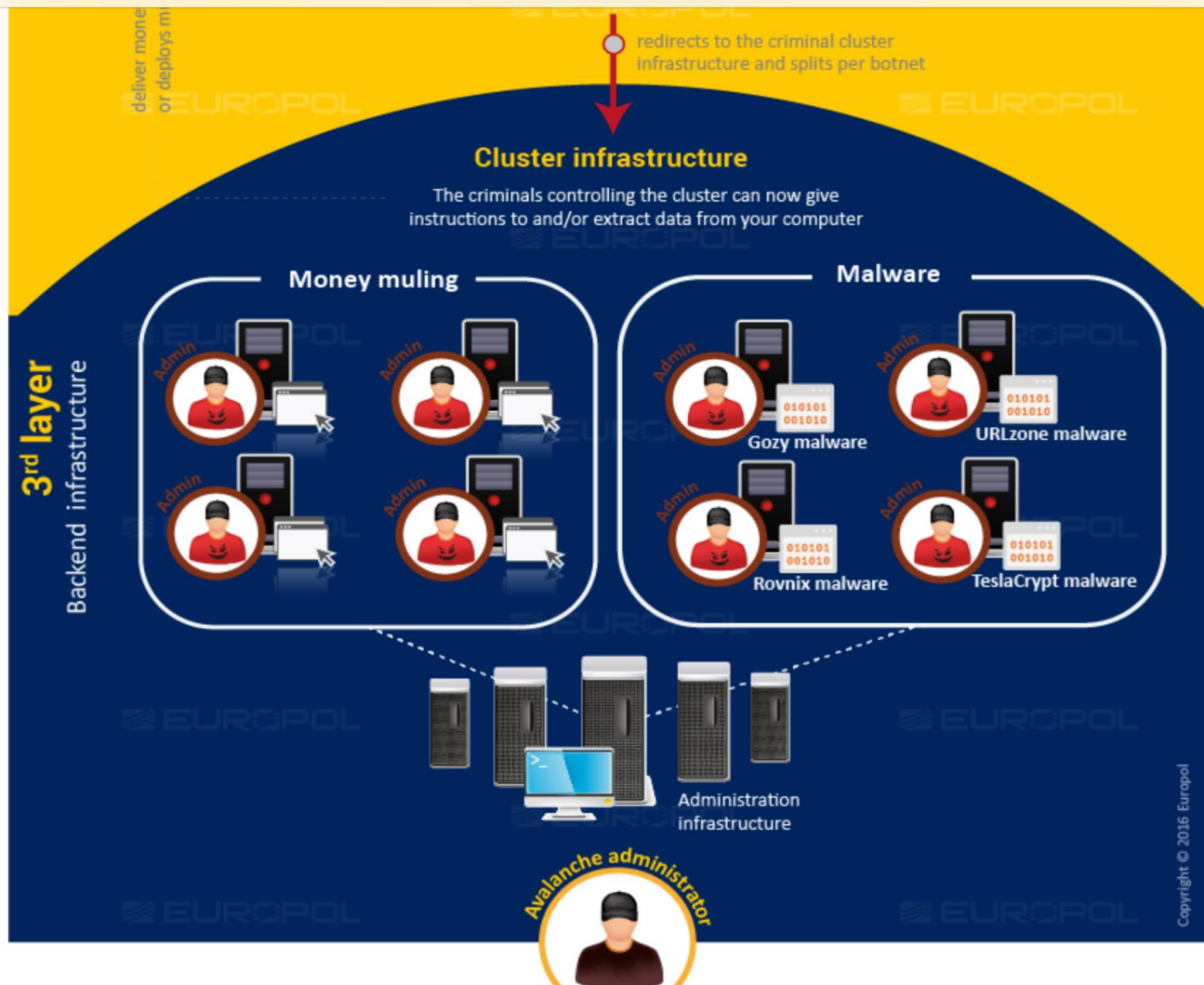


iPad

16:17

europol.europa.eu

76%







# Sinkholing

is an action whereby traffic between infected computers and a criminal infrastructure is redirected to servers controlled by law enforcement authorities and/or an IT security company. This may be done by assuming control of the domains used by the criminals or IP addresses.

When employed at a 100% scale, infected computers can no longer reach the criminal command and control computer systems and so criminals can no longer control the infected computers.

The sinkholing infrastructure captures victims' IP addresses, which can subsequently be used for notification and follow-up through dissemination to National CERTs and Network Owners.





## Prosecutor's Office Paid Bitcoin Ransom in Cyberattack

By JOE MANDAK, ASSOCIATED PRESS ·  
PITTSBURGH — Dec 5, 2016, 6:56 PM ET

 Share with Facebook

 Share with Twitter

### SHARE



A state prosecutor's office in Pennsylvania was among hundreds of thousands of victims of a now-shuttered international cybercrime operation, paying nearly \$1,400 in a [bitcoin](#) ransom to free up its infected computer network, authorities disclosed Monday.



Federal prosecutors said in court documents only that an unidentified state government entity had been victimized by the ring known as the [Avalanche](#) network. But the Allegheny County district attorney, Stephen Zappala Jr., confirmed to The Associated Press that it was his office.



The disabling of the Avalanche network by the European Union and U.S. authorities was announced last week in Europe. Federal documents unsealed in Pittsburgh on Monday provided additional details.

The Avalanche group had operated since at least 2010 and infected at least 500,000 computers worldwide, said Soo Song, acting U.S. Attorney in Pittsburgh.

"The takedown of Avalanche was unprecedented in its scope, scale, reach and level of cooperation among 40 countries," Song said.





## Feds: Business lost \$387,500 in world cybercrime operation

December 5, 2016 by Joe Mandak



Credit: George Hodan/Public Domain

A Pennsylvania business lost more than \$387,000 in an international cybercrime operation disabled by federal authorities and the European Union last week.

[Create, deploy, and manage fully customizable simulation apps with COMSOL Multiphysics and the Application Builder](#)  
Learn more here: [www.comsol.com](http://www.comsol.com)

Federal prosecutors and FBI agents in Pittsburgh on Monday plan to offer more details from last week's sweep of the Avalanche network. The group is accused of inflicting hundreds of millions of dollars in losses worldwide before it was dismantled and five key suspects were arrested.

Documents unsealed Monday show a business in Carnegie lost \$387,500 when someone drained the money from the company's online account.

Another business in New Castle was twice targeted with unsuccessful efforts to steal more than \$120,000.

The U.S. Department of Justice has accused the network of hosting some of the world's most pernicious malware as well as several money laundering campaigns.

➦ **Explore further:** Police make 5 arrests in 'unprecedented' cybercrime takedown





## What challenges involved in Avalanche Operation?

- Where were the servers?
- Where were the perpetrators?
- Who were the perpetrators?
- What damage was done?
- What malware used?
- Who to lead investigation?
- Who & where were the victims?
- What format is needed for required evidence?
- How identify investigative partners?
- How to request required evidence?
- How disable/delete the malware?
- Who & where to prosecute?
- What evidence required?
- Where is the required evidence?





# Operation Avalanche

**Issues breakdown into:**

- ❖ **Legal**
- ❖ **Procedural**
- ❖ **Practical**

**What about?**

- ❖ **Political?**
- ❖ **Economic?**
- ❖ **Cultural?**



# **Case Study: Axact – Global Diploma Mill**



## Fake Diplomas, Real Cash: Pakistani Company Axact Reaps Millions

By DECLAN WALSH MAY 17, 2015

602 COM



Axact, which has its headquarters in Karachi, Pakistan, ostensibly operates as a software company.  
Sara Farid for The New York Times

**EDTECH SEMINAR**  
16 - 17 November 2015  
The Ritz Carlton Hotel, DIFC, Dubai, UAE

**FREE TO ATTEND**  
LOOKING FOR THE LATEST TECHNOLOGY TO TRANSFORM YOUR TEACHING OUTCOME?

**BOOK YOUR SEAT NOW!**

Email

Share

Tweet

Save

More

**BROOKLYN**  
NOW PLAYING

Seen from the Internet, it is a vast education empire: hundreds of universities and high schools, with elegant names and smiling professors at sun-dappled American campuses.

Their websites, glossy and assured, offer online degrees in dozens of disciplines, like nursing and civil engineering. There are glowing endorsements on the [CNN iReport](#) website, enthusiastic video testimonials, and State Department authentication certificates bearing the signature of Secretary of State John Kerry.

"We host one of the most renowned faculty in the world," boasts a woman introduced in [one promotional video](#) as the head of a law school. "Come be a part of Newford University to soar the sky of excellence."



## **Take down of a Global Organized Crime Syndicate**

- **Swift Action**
- **Over 700 TB of data**
- **Over 14,000 websites**
- **Legal entities all over the world**
- **Cross-border money trails**
- **Protecting US, UK, Australia, UAE, Saudi  
and other citizens and Governments**



## Degree Shipped To Different Countries

Country Name	Total
Afghanistan	135
Aland Islands	1
Albania	28
Algeria	78
American Samoa	4
Andorra	1
Angola	152
Morocco	40
Mozambique	32
Myanmar	43
Namibia	19
Nauru	7
Nepal	29
Netherlands	241
Netherlands Antilles	7
New Zealand	73
Nicaragua	3
Niger	19
Nigeria	461



U-2015-4-117750	Nicholson University	Agha Abani	agha.abani@harrybeat.com	NIGERIA	#6 Railway Close, Behind Nitel, D/Line Port Harcourt P.O. Box 10068, Mile 1 Diobu Port Harcourt, Rivers State Nigeria		Nigeria	Nigeria	4/29/2015	399	UNITED ARAB EMIRATES	
D-2006-12-27526	Rochville University	Jimmy L Decker	jidecker@swbell.net	NIGERIA	kelvin street no.11		kaduna	NEW YORK	6/6/2005	629	NULL	
D-2006-12-28890	Rochville University	Patricia A Farmer	babytaz082502@yahoo.com	NIGERIA	12 AKEMU STREET, OKUMAGBA LAYOUT WARRI, DELTA STATE, NIGERIA.		WARRI	DELTA STATE, WARRI.	5/1/2005	399	NULL	
D-2006-12-36571	Rochville University	Fatade Shade	timtoners@yahoo.com	NIGERIA	48, suenu road off gbaja market		surulere	Lagos State	2/15/2005	2528	NULL	
D-2006-12-27351	Rochville University	EZOKE, MARK IGIRI	ezokemark@yahoo.co.vk	NIGERIA	29, Shipeolu Street, Palm Grove		Shomolu	MARYLAND	4/5/2005	99	NULL	
U-2006-12-8165	Ashwood University	NNewuihe Benigrous Obinna	japhet_ekpo@yahoo.ca	NIGERIA	4 odukoya street off odunsi		bariga	lagos	10/9/2006	1438	NULL	2348



AD-2006-12127351	Rochville University	EZOKE, MARK IGIRI	ezokemark@yahoo.co.vk	NIGERIA	29, Shipeolu Street, Palm Grove		Shomolu	MARYLAND	4/5/2005	99	NULL	
AU-2006-1298165	Ashwood University	NNewuihe Benigrous Obinna	japhet_ekpo@yahoo.ca	NIGERIA	4 odukoya street off odunsi		bariga	Iagos	10/9/2006	1438	NULL	234
AU-2007-11124808	Ashwood University	Thomas Yates	thomas.yates2@us.army.mil	NIGERIA	AGBARA PRODUCTION PLATFORM, AGIP ENERGY & NAT. RESOURCES NIG. LTD., MILE 4 NEW-BASE, PO BOX 923 PORT-HARCOURT.		PORT - HARCOURT,	RIVERS - STATE	11/17/2007	99	NULL	
BU-2007-9-405074	Belford University	omokafe tokura	blaze4iamp@yahoo.com	NIGERIA	2nd floor A.P plaza, Aminu Kanu crescent, wuse 2 Abuja, Nigeria		Abuja	Abuja	9/26/2007	1477	NULL	
AD-2006-12230061	Rochville University	Verna Philmon Young	vyathome@yahoo.com	NIGERIA	NO 10 NEW HEAVEN		ENUGU	NEBRASKA	6/10/2005	1438	NULL	





AD-2006-12302654	Rochville University	Uge Franklin Oghenekewe	frankuge@tyahoo.com	NIGERIA	Block S 5 Flat 3 Sam Ethnan Base		Ikeja	Lagos	8/18/2006	579	NULL	
AD-2006-12223685	Rochville University	matthew williams	mjwchevy@isp.com	NIGERIA	NO 6, ARTHUR MBACHU STREET MAJIYAGBE		IPAJA	LAGOS	7/20/2007	99	NULL	
AD-2006-1292898	Rochville University	alejandro moreno alvarez	judgejls@yahoo.co.uk	NIGERIA	38 Lake Chad Crescent,		Abuja	AMAC, FCT	10/11/2004	289	NULL	
AD-2006-9-307831	Rochville University	Adesoji Adesoji D.	solventcomputer@yahoo.com2	NIGERIA	No 9 Okunola Abass street, New Bodija		Ibadan	Oyo State	9/19/2006	918	NULL	
BU-2006-8-392441	Belford University	Adebola A A	caotaincode@yahoo.com	NIGERIA	P.O. Box 2531Garki		FCT	Abuja	8/14/2006	374	NULL	



AMUO-2014-08-111439	Almeda University Online	Michael Olu	olumus@yahoo.co.uk1	NIGERIA	Pastor Olu Compound, Lubey Agbeta, Onne	Port Harcourt	Port Harcourt	Rivers State	9/9/2014	1500	NULL	###
AMUO-2014-09-111524	Almeda University Online	Michael Olu	olumus@yahoo.co.uk2	NIGERIA	Pastor Olu Compound, Lubey Agbeta, Onne		Port Harcourt	Rivers State	9/10/2014	500	NULL	###
AD-2006-9-307831	Rochville University	Adesoji Adesoji D.	solventcomputer@yahoo.com2	NIGERIA	No 9 Okunola Abass street, New Bodija		Ibadan	Oyo State	9/19/2006	918	NULL	
AU-2006-12-53228	Ashwood University	Christian Ekeocha	bertvisionconsulting20202000@yahoo.co.uk	NIGERIA	10 Afeez Street, Ilasa		Ilasa Mushin	Lagos State	5/27/2006	419	NULL	0+2:666
AD-2006-12-229196	Rochville University	RICK MARTINEZ	trc003@qwest.net	NIGERIA	St. Patrick's Catholic Church, Ikot Ansa, PO Box 2908,	NULL	Calabar	NON US	4/4/2005	399	NULL	



- Pakistan not a member of:
  - Warsaw Convention
  - Budapest Convention
- No mechanism for cross-border exchange of electronic evidence and financial trails
- Innovation was the only option to successfully cooperate internationally, pursue case and freeze assets

## Spontaneous Information

- Request submitted to FBI for information resulted in so much information that the request in effect became spontaneous interagency information sharing
- Enabled FBI to initiate its investigation and ultimately send letter to FIA that was to be used as evidence in court



- Law enforcement agency cooperated directly with US Federal Trade Commission
- Cross border exchange – data had to be sent on physical storage devices (equivalent to over 10,000 pages of data)
- Received prompt response after FTC conducted its internal investigation based upon data provided to it



UNITED STATES OF AMERICA <b>FEDERAL TRADE COMMISSION</b> WASHINGTON, DC 20580		Return this form to: Federal Trade Commission Office of International Affairs 600 Pennsylvania Ave., NW Washington, DC 20580
<b>Foreign Law Enforcement Agency Request for Investigative Assistance</b>		
Pursuant to the Federal Trade Commission Act, 15 U.S.C. §§ 41 et seq., and Rules 4.10(d) and 4.11(j) of the FTC Rules of Practice, 16 C.F.R. §§ 4.10(d) and 4.11(j), I hereby request the investigative assistance described below:		
1. FTC Staff Contact: <input type="text"/>		
2. Foreign Law Enforcement Agency Contact: <input type="text"/>		
3. Indicate the area(s) in which your agency has law enforcement or investigative authority: <input type="checkbox"/> civil matters <input type="checkbox"/> criminal matters <input type="checkbox"/> administrative matters		
4. Identify the source of your agency's law enforcement or investigative authority: <input type="text"/>		
5. Provide a brief description of your agency: <input type="text"/>		
6. What kind of law violation or crime are you investigating or prosecuting? <input type="text"/>		



## Cross-border Cooperation with Private Sector

- Exchange of data between FIA and Michigan private attorneys resulted in quicker freezing of assets abroad
- No need to go to Pakistan MoFA and Embassy to US DoS, DoJ and FBI
- Michigan attorneys provided corporate data available to them,

### Belford High School Class Action Website

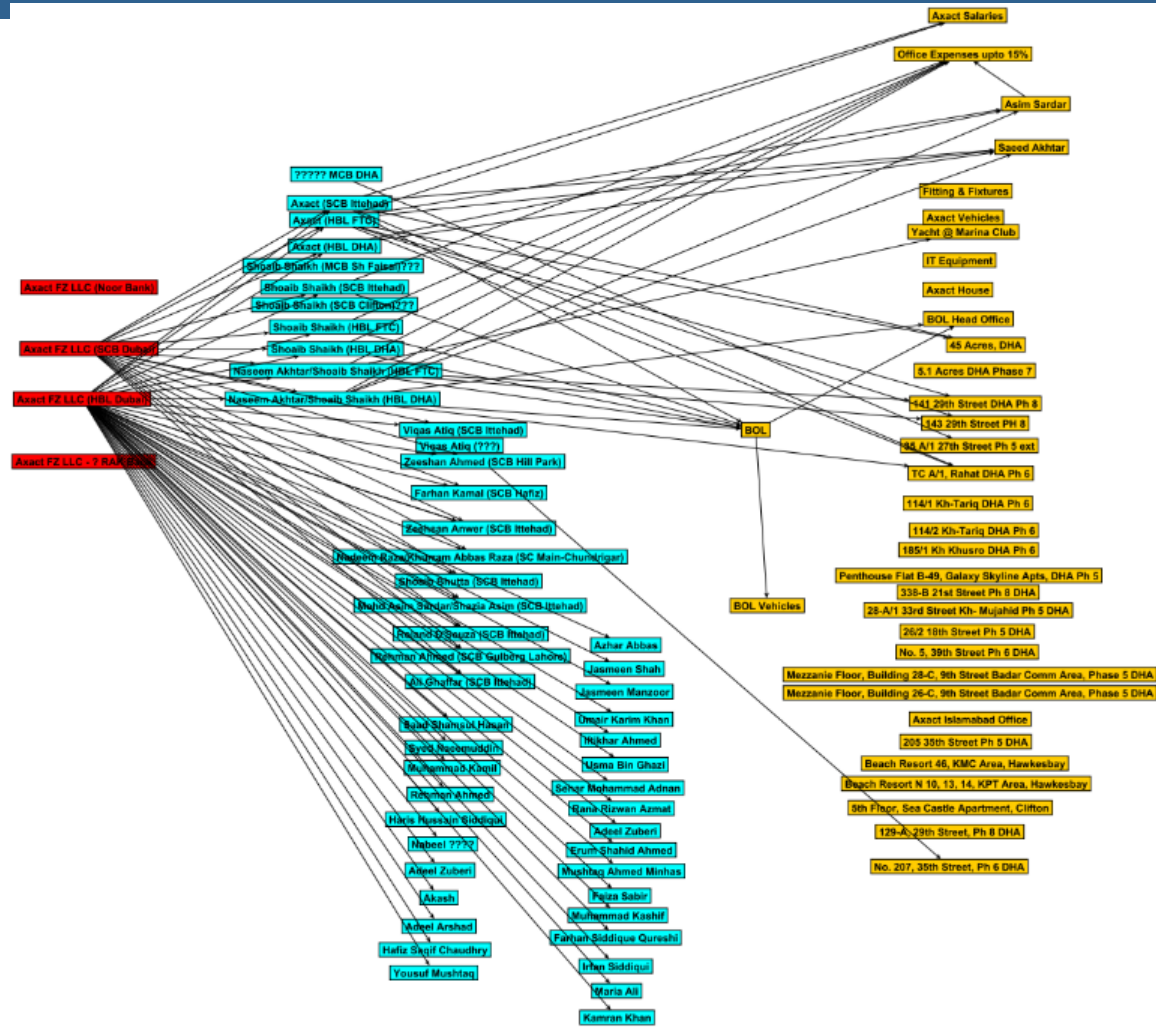
[www.belfordclassaction.com](http://www.belfordclassaction.com)

On August 31, 2012, Belford High School, Belford University and a host of their co-conspirators were ordered to pay more than \$22.7 million to the victims of their scams, a class of more than 30,000 U.S. residents who were duped into purchasing fake high school diplomas from Belford. The judgment established the truth of allegations that Belford High School and Belford University are fake schools that do not actually exist.

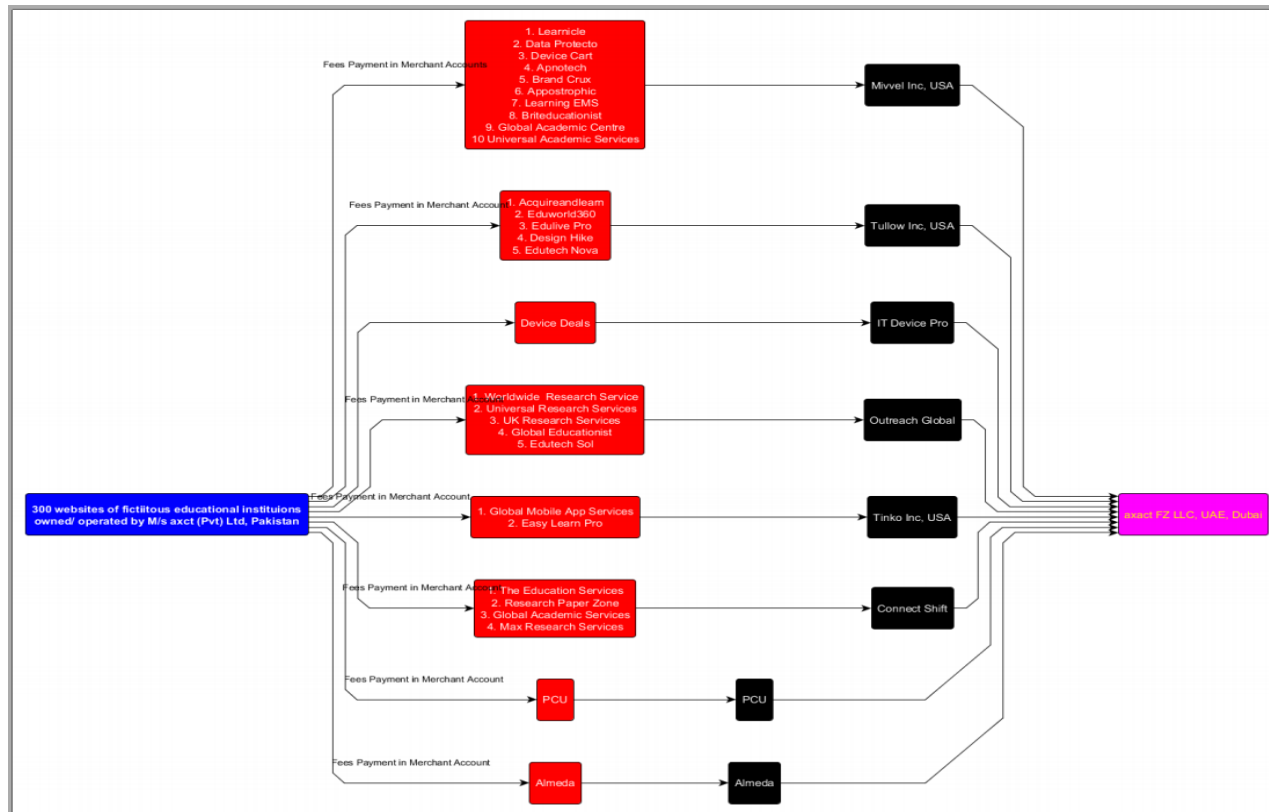
Belford was also ordered to forfeit the websites used to perpetrate its scam, including [www.belfordhighschool.com](http://www.belfordhighschool.com), [www.belfordhighschool.org](http://www.belfordhighschool.org), [www.belforduniversity.org](http://www.belforduniversity.org), and [www.belforduniversity.com](http://www.belforduniversity.com). These scam websites have now been taken down so they can no longer harm consumers.

These significant developments come as a result of extensive efforts that have occurred since the case was filed in November 2009 by The Googasian Firm, P.C., a Michigan-based law firm appointed by the federal court to represent the class of more than 30,000 U.S. residents who were victimized by Belford's scam. For a timeline of significant events and rulings relating to the litigation and Belford High School, [click here](#).

The lawsuit, filed on November 5, 2009, alleged that Belford High School is an internet scam that defrauds students of their money. The lawsuit alleged that Belford High School takes students' money by offering them a supposedly "valid" and "accredited" high school diploma, but that the school is fake and the diplomas are not valid. The lawsuit alleged that the two accrediting agencies by which Belford claimed to be accredited – International Accreditation Agency for Online Universities and the Universal Council for Online Education Accreditation – are not legitimate accrediting agencies. The lawsuit alleged that these two accrediting agencies, like Belford, are fake. The judgment entered by the Court confirmed these facts as true. From July 2010 to October 2011, Belford was represented by The Miller Law Firm of Rochester, Michigan. The Miller Law Firm opposed class certification on behalf of Belford during its period of representation, but the Court rejected the arguments made on behalf of Belford and certified the case as a class action.







UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF MICHIGAN

CARRIE MCCLUSKEY, et al.,

Plaintiffs,

Case No. 4:09-cv-14345-MAG-MKM

Hon. Mark A. Goldsmith

v.

BELFORD HIGH SCHOOL, et al.,

Defendants.

---

**DECLARATION OF SHOAIB SHAIKH**

Shoaib Shaikh, declares as follows:

1. I am more than 18 years of age and am competent to make this declaration.
2. I am a director of Garnishee Defendants Tullow, Inc. and Tinko, Inc. ("Garnishee Defendants").
3. I make this Declaration based on personal knowledge.
4. Garnishee Defendants are Delaware companies that provide global online payment processing services as resellers/billing providers for online businesses (similar to 2checkout.com).

5. Garnishee Defendants have no employees, offices or property in the State of Michigan.

6. I am responsible for the Garnishee Defendants' operations, which are automated services. When I needed to perform work for the Garnishee Defendants, I did that work from my home or office in Pakistan. Any technical work was outsourced to Axact FZ LLC in United Arab Emirates when needed.

7. Currently, and for approximately the past nine months, I have been detained by Pakistani law enforcement authorities and am in their custody.

8. As a result of being detained by Pakistani law enforcement authorities, I am not permitted to travel to the United States for any depositions noticed by Plaintiffs in the above captioned matter. I also would not be able to obtain a Visa to travel to the United States.

9. I am the most knowledgeable person to testify as a corporate representative on behalf of Garnishee Defendants regarding the operations of Garnishee Defendants and the topics identified in any depositions noticed by Plaintiffs of Garnishee Defendants in the above captioned matter.

10. Even if I could travel, it would be unduly burdensome and costly to travel to Michigan for the noticed depositions.



FIR No. 7 of 2015 - dated 27.05.2015

(State vs. M/s. Axact (Pvt) Ltd.) - FIA, Corporate Crime Circle, Karachi

With reference to the above noted matter, the ongoing investigation has revealed substantial crucial evidence that is outside Pakistan which requires Request for Legal Assistance from the US Department of Justice in general and the Office of International Judicial Assistance, in particular and Federal Bureau of Investigation for the following:

1. Request that digital evidence which is at risk of destruction and removal (through erasure/deletion) and hence volatile requiring urgent action through cooperation on the part of the US Government and law enforcement be secured, preserved and transmitted as evidence to Pakistan to aid the investigation and prosecution of the above noted matter (details of service providers and the data to be preserved and other details enumerated in Annex A)
2. Assistance in recording statements of customers/victims (contact details listed at Annex B)
3. Request confirmation/corroboration of the inauthenticity of the degrees/accreditations/diplomas/certifications suspected to be or identified as fake, fraudulent and forged, that have been issued by the non-existent educational and other institutions through the use of "spoofed" inauthentic, fraudulent and forged websites (details enumerated in Annex C)
4. Request verification of corroboration of the authenticity or inauthenticity, as the case may be of suspected fake, fraudulent, forged and inauthentic legalizations, attestations, notarizations, apostilles, seals and approvals attributed to the US Department of State, US Government and Notaries. (details enumerated in Annex D)
5. Request verification of corroboration of the authenticity or inauthenticity, as the case may be of suspected fake, fraudulent, forged and inauthentic Schools and Universities. (details enumerated in Annex DD)
6. Request disclosure of the bank account statements for each bank account identified in Annex E from the time of its opening until 30th July 2015 or at least initially statements for the last 7 years

10. Request information and details of the shareholding and identity of the shareholders, directors, officers, company secretaries, any authorized signatories for or on behalf of legal entities identified in Annex F along with, if available, the nationality(s), address(es), any contact details or other details that may be available with respect to the aforesaid persons
11. Request that the prosecution be permitted to present the information and documents received before the competent courts in Pakistan in connection with the criminal proceedings and ancillary proceedings regarding the proceeds of crime and money laundering, unless otherwise specified
12. Request the provision of the transcripts, pleadings, orders, judgments and records of the proceedings before the United States District Court Eastern District Of Michigan Southern Division in Civil Action No. 09-CV-14345 ELIZABETH LAUBER, et al., vs. BELFORD HIGH SCHOOL, et al., (<http://www.belfordlawsuit.com/>)
13. Assistance between prosecutorial/investigative team leads and their counterparts on an ongoing basis with respect to this case

The undersigned requests that necessary urgent cooperation and assistance in this criminal matter may kindly be sought from the foreign Governments, law enforcement authorities as well as corporations/businesses to aid the investigation. This office is also willing and able to provide any assistance for the preparation of such requests given the complexity, volume and countries involved as may be deemed necessary by the competent authority.

Submitted for your kind consideration and urgent approval.

UNCLASSIFIED//REL TO USA, PAK



Memorandum

File No. IS-C163-A  
NY-6434502

Office of the Legal Attaché  
United States Embassy  
Islamabad, Pakistan

8 February 2016

Office of the Director  
FIA Islamabad Zone  
Express Way-Iqbal Town  
Islamabad, Pakistan

(U//REL TO USA, PAK) As your Service is aware, the FBI has been investigating a Pakistan-based entity named Axact. Ongoing investigation has identified a "diploma mill", orchestrated by Axact, and headquartered in Karachi, Pakistan. Among engaging in other nefarious activity, Axact's primary scheme of illegality pertains to soliciting the sale of fictitious college and high school diplomas to both witting and unwitting purchasers. The vast majority of purchasers have been identified as located both within the United States and throughout the Middle East.

(U//REL TO USA, PAK) In furtherance of this scheme, Axact has established a worldwide web of shell companies and associates. The shell companies have been used to veil Axact funds and proceeds, to further facilitate the transport of the fictitious diplomas, as well as to enhance the illusion that the diplomas were from legitimate educational institutions (e.g., via securing fictitious accreditation either within the United States or abroad).

(U//REL TO USA, PAK) Regarding financial accounts located in the United States, Axact appears to have set up three primary shell companies in the United States, by the names of Mivvel Inc., Tullow Inc., and Tinko Inc., as well as various tertiary shell companies, to include, but not limited to Blitzace Inc. The Directors of said entities have been identified to include both Pakistani-based Axact executives, as well as United States-based individuals.

(U//REL TO USA, PAK) Viquez Atiq, the Chief Operating Officer of Axact, holds 49% of the shares of Mivvel Inc. Shoaib Ahmed, and the Owner/President of Axact, holds 49% of the shares of Tullow and Tinko. With respect to Mivvel Inc., the remaining 51% of the shares belong to Ali Gaffar Vyajkora, date of birth 23 March 1971, 109 Juliett Fowler Street, # B-303, Dallas, Texas.

(U//REL TO USA, PAK) With respect to Tinko and Tullow, the majority share holders are Zubair Syed (Tullow), date of birth 27 October 1962, and Uzma Shaheen (Tinko), date of birth 7

D12/NR3C/MISC/2016/1878  
Dated 17/2/16



Being able to demonstrate:

- best practice procedures/processes were in place
- responsibilities were allocated
- assisted in information exchange and led to greater international cooperation, for instance, from:
  - Michigan lawyers
  - FBI
  - FTC









# Budapest Convention on Cybercrime

## International co-operation tools

- Operational and procedural rules
- Common to other international conventions
- Some of them, very innovative



# Mutual Legal Assistance



# Budapest Convention on Cybercrime

- Default
- Extradition
- Legal Mutual Assistance
- Spontaneous Information
- Confidentiality and limitation on use
- Expedited preservation of stored computer data
- Expedited disclosure of preserved traffic data
- Mutual assistance regarding
  - accessing of stored computer data
  - access to real-time collection of traffic data
  - interception of content data
- 24/7 Network
- Trans border Access



## Fake Diplomas, Real Cash: Pakistani Company Axact Reaps Millions

By DECLAN WALSH MAY 17, 2015

602 COMMENTS



Axact, which has its headquarters in Karachi, Pakistan, ostensibly operates as a software company.  
Sara Farid for The New York Times

**EDTECH SEMINAR**  
16 - 17 November 2015  
The Ritz Carlton Hotel, DIFC, Dubai, UAE

**FREE TO ATTEND**  
LOOKING FOR THE LATEST TECHNOLOGY TO TRANSFORM YOUR TEACHING OUTCOME?

**BOOK YOUR SEAT NOW!**

Email

Share

Tweet

Save

More



Seen from the Internet, it is a vast education empire: hundreds of universities and high schools, with elegant names and smiling professors at sun-dappled American campuses.

Their websites, glossy and assured, offer online degrees in dozens of disciplines, like nursing and civil engineering. There are glowing endorsements on the [CNN iReport](#) website, enthusiastic video testimonials, and State Department authentication certificates bearing the signature of Secretary of State John Kerry.

"We host one of the most renowned faculty in the world," boasts a woman introduced in [one promotional video](#) as the head of a law school. "Come be a part of Newford University to soar the sky of excellence."



# Budapest Convention on Cybercrime

## Spontaneous information disguised as MLA request

FIR No. 7 of 2015 - dated 27.05.2015

(State vs. M/s. Axact (Pvt) Ltd.) - FIA, Corporate Crime Circle, Karachi

With reference to the above noted matter, the ongoing investigation has revealed substantial crucial evidence that is outside Pakistan which requires Request for Legal Assistance from the US Department of Justice in general and the Office of International Judicial Assistance, in particular and Federal Bureau of Investigation for the following:

1. Request that digital evidence which is at risk of destruction and removal (through erasure/deletion) and hence volatile requiring urgent action through cooperation on the part of the US Government and law enforcement be secured, preserved and transmitted as evidence to Pakistan to aid the investigation and prosecution of the above noted matter (details of service providers and the data to be preserved and other details enumerated in Annex A)
2. Assistance in recording statements of customers/victims (contact details listed at Annex B)
3. Request confirmation/corroboration of the inauthenticity of the degrees/accreditations/diplomas/certifications suspected to be or identified as fake, fraudulent and forged, that have been issued by the non-existent educational and other institutions through the use of "spoofed" inauthentic, fraudulent and forged websites (details enumerated in Annex C)
4. Request verification of corroboration of the authenticity or inauthenticity, as the case may be of suspected fake, fraudulent, forged and inauthentic legalizations, attestations, notarizations, apostilles, seals and approvals attributed to the US Department of State, US Government and Notaries. (details enumerated in Annex D)
5. Request verification of corroboration of the authenticity or inauthenticity, as the case may be of suspected fake, fraudulent, forged and inauthentic Schools and Universities. (details enumerated in Annex DD)
6. Request disclosure of the bank account statements for each bank account identified in Annex E from the time of its opening until 30th July 2015 or at least initially statements for the last 7 years

10. Request information and details of the shareholding and identity of the shareholders, directors, officers, company secretaries, any authorized signatories for or on behalf of legal entities identified in Annex F along with, if available, the nationality(s), address(es), any contact details or other details that may be available with respect to the aforesaid persons
11. Request that the prosecution be permitted to present the information and documents received before the competent courts in Pakistan in connection with the criminal proceedings and ancillary proceedings regarding the proceeds of crime and money laundering, unless otherwise specified
12. Request the provision of the transcripts, pleadings, orders, judgments and records of the proceedings before the United States District Court Eastern District Of Michigan Southern Division in Civil Action No. 09-CV-14345 ELIZABETH LAUBER, et al., vs. BELFORD HIGH SCHOOL, et al., (<http://www.belfordlawsuit.com/>)
13. Assistance between prosecutorial/investigative team leads and their counterparts on an ongoing basis with respect to this case

The undersigned requests that necessary urgent cooperation and assistance in this criminal matter may kindly be sought from the foreign Governments, law enforcement authorities as well as corporations/businesses to aid the investigation. This office is also willing and able to provide any assistance for the preparation of such requests given the complexity, volume and countries involved as may be deemed necessary by the competent authority.

Submitted for your kind consideration and urgent approval.

# Budapest Convention on Cybercrime

## Spontaneous information disguised as MLA request

UNCLASSIFIED//REL TO USA, PAK

Memorandum

File No. IS-C163-A  
NY-6434502

Office of the Legal Attaché  
United States Embassy  
Islamabad, Pakistan

8 February 2016

Office of the Director  
FIA Islamabad Zone  
Express Way-Iqbal Town  
Islamabad, Pakistan

(U//REL TO USA, PAK) As your Service is aware, the FBI has been investigating a Pakistan-based entity named Axact. Ongoing investigation has identified a "diploma mill", orchestrated by Axact, and headquartered in Karachi, Pakistan. Among engaging in other nefarious activity, Axact's primary scheme of illegality pertains to soliciting the sale of fictitious college and high school diplomas to both witting and unwitting purchasers. The vast majority of purchasers have been identified as located both within the United States and throughout the Middle East.

(U//REL TO USA, PAK) In furtherance of this scheme, Axact has established a worldwide web of shell companies and associates. The shell companies have been used to veil Axact funds and proceeds, to further facilitate the transport of the fictitious diplomas, as well as to enhance the illusion that the diplomas were from legitimate educational institutions (e.g., via securing fictitious accreditation either within the United States or abroad).

(U//REL TO USA, PAK) Regarding financial accounts located in the United States, Axact appears to have set up three primary shell companies in the United States, by the names of Mivvel Inc., Tullow Inc., and Tinko Inc., as well as various tertiary shell companies, to include, but not limited to Blitzace Inc. The Directors of said entities have been identified to include both Pakistani-based Axact executives, as well as United States-based individuals.

(U//REL TO USA, PAK) Viqas Atiq, the Chief Operating Officer of Axact, holds 49% of the shares of Mivvel Inc. Shoaib Ahmed, and the Owner/President of Axact, holds 49% of the shares

Handwritten notes and signatures on the right margin include: "S.I. Hakeem", "For v/a + reports", "2/16", "2/17", and "NR3C/MISC/2016/1878".





# Budapest Convention on Cybercrime

## Article 26

### Spontaneous Information

1 - A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.





# Budapest Convention on Cybercrime

## Article 26 Spontaneous Information

2 - Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.



# Budapest Convention on Cybercrime

## Spontaneous Information

- The authorities from a Party, within an internal investigation, discover that some of the information they obtained must be forwarded to the authorities of other Party
- It can be done if the information seems to be useful or necessary to the beginning or the developing of an investigation respecting to a criminal offence in the framework of the Convention
- According to Article 26, 2, this dispatch of information can be submitted to certain conditions, mainly of confidentiality



# Budapest Convention on Cybercrime

## Article 29

### Expedited Preservation of Stored Computer Data

- 1 - A Party may request another Party to **order or otherwise obtain the expeditious preservation of data stored by means of a computer system**, which is located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.



# Budapest Convention on Cybercrime

## Article 29

- **Expedited preservation** of data stored in a computer system
- Parallel framework to the internal provision
  - allows one contracting Party to require from other Party the expedited preservation of data
  - if at the same time expresses its intention of sending a formal request of assistance for a search, or a seizure, or any similar measure
- The requested party must act with due diligence, to preserve requested data, according to its own national law
- Dual criminality cannot be required by the requested party, as condition for preservation of data (*except offenses other than Art 2-11 or political, sovereignty, security, public order, or other essential interests*)



# Budapest Convention on Cybercrime

## Requesting Expeditious Preservation

- Specify:
  - Authority seeking preservation
  - Offence that is subject of criminal investigation
  - Brief summary of facts of case
  - Stored computer data to be preserved
  - Any available information on custodian of data or location of computer system
  - Necessity of preservation
  - That party intends to submit request for MLA



# Budapest Convention on Cybercrime

## Requesting Expeditious Preservation

- Grounds for refusals:
  - Dual criminality only if party requires dual criminality as condition for responding to other mutual legal assistance requests and believes that condition will not be met (*i.e. offenses other than Art 2-11*)
  - Request in relation to political offence
  - Execution of request will prejudice sovereignty, security, ordre public or other essential interests
- Period of preservation – at least 60 days



# Budapest Convention on Cybercrime

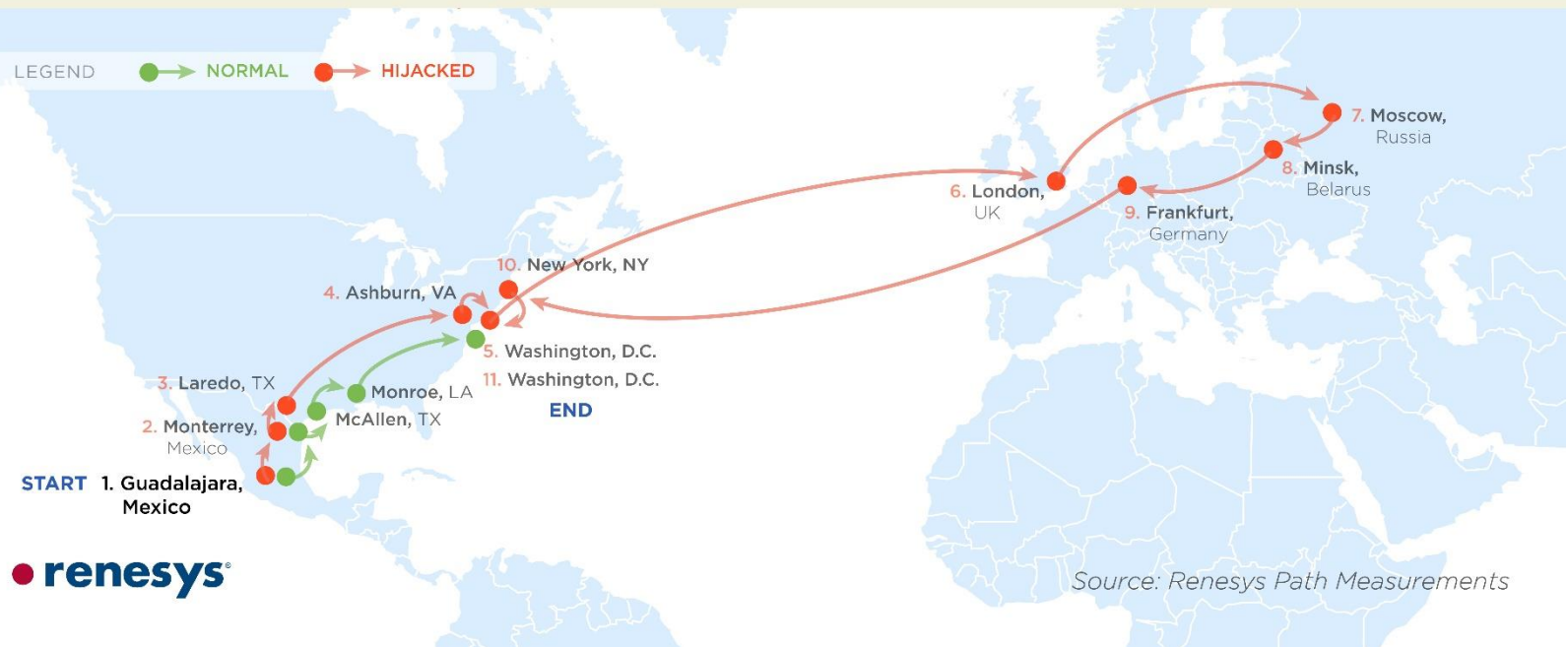
## Article 30

### Expedited Disclosure of Preserved Traffic Data

1. Where, in the course of the execution of a request made under Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data in order to identify that service provider and the path through which the communication was transmitted.

# Budapest Convention on Cybercrime

## Traceroute Path 1: from Guadalajara, Mexico to Washington, D.C. via *Belarus*







# Budapest Convention on Cybercrime

## Requesting partial disclosure of traffic data

- Disclosure of sufficient amount of traffic data be provided to identify service provider and path of a communication
- Disclosure may be withheld if:
  - Request in relation to political offence
  - Execution of request will prejudice sovereignty, security, *ordre public* or other essential interests



# Budapest Convention on Cybercrime

## Article 31 - Mutual Assistance Regarding Accessing of Stored Computer Data

- Request to another State to search or seize (and disclose) data stored by means of a computer system
  - Located within the territory of the requested State
  - Including data that has been preserved pursuant to Article 29
- [A.23 instruments]



# Budapest Convention on Cybercrime

## Article 31 - Mutual Assistance Regarding Accessing of Stored Computer Data

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29

2. (Ability of the requested party to do so)



# Budapest Convention on Cybercrime

## Article 31 - Mutual Assistance Regarding Accessing of Stored Computer Data

3. The request shall be responded to on an expedited basis where:

- (a) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
- (b) the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.



# Budapest Convention on Cybercrime

## Requesting access to stored data

- Request to search, similarly access, seize or similarly secure
- For expedited response:
  - request should have grounds that data is particularly vulnerable to loss or modification
  - MLAT and laws should allow for responding on expeditious basis



# Budapest Convention on Cybercrime

## Article 32 – Transborder Access

- Possibility given to law enforcement from a Party to obtain evidence stored in a computer physically located in other Party's territory
  - Without any request of international cooperation if, during a concrete investigation, the officers in charge
    - need to obtain open source information from a computer located in a foreign country ;
- or*
- access data with the lawful and voluntary consent of the lawfully authorised person



# Budapest Convention on Cybercrime

## Article 32 – Transborder Access to Stored Computer Data with Consent or Where Publicly Available

A Party may, without the authorisation of another Party:

a)- access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b) - access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.





# Budapest Convention on Cybercrime

**Two other data categories:**

❖ **Open source**

❖ **Publicly available**

**G8**

**Principles on Transborder Access to Stored  
Computer Data  
(Moscow 1999)**



# Budapest Convention on Cybercrime

## **Public/Open Source Data:**

Can be accessed by anyone and used as evidence even though 'located' in another country



# Budapest Convention on Cybercrime

## **Private/Protected Data:**

Access restricted to authorised persons (need log-in credentials).



# Budapest Convention on Cybercrime

## Article 33 - Mutual Assistance Regarding Real Time Collection of Traffic Data

1. The Parties shall provide mutual assistance to each other with respect to the **real-time collection of traffic data** associated with **specified communications** in its territory transmitted by means of a computer system. Subject to paragraph 2, assistance shall be governed **by the conditions and procedures provided for under domestic law**.

2. Each Party shall **provide such assistance** at least with respect to criminal offences for which real-time collection of traffic data would be available **in a similar domestic case**.



# Budapest Convention on Cybercrime

## Article 34

### Mutual assistance regarding the interception of content data

- Mutual assistance in the real-time collection or recording of content data of specified communications transmitted by means of a computer system
- to the extent permitted under their applicable treaties and domestic laws.



# Budapest Convention on Cybercrime

## Article 35

### 24/7 Contact Points

- Obligation to create a permanently available contact point
  - a so called *24/7 network* of contact points
- General objectives of these contact points
  - to facilitate international co-operation
  - giving **technical advisory** to other contact points
  - **activating** the proper mechanism to expedited **preservation** of data
  - **urgently collecting** evidence
  - **identifying and discovering** suspects



# Budapest Convention on Cybercrime

## Article 35

### 24/7 Contact Points

- Operational network of experts on high-tech criminality
- Provide help and cooperation very quickly even if a formal cooperation request must follow this informal way
- One single point of contact for each country, available 24 hours a day, 7 days a week
- Direct communications between the points
- Mainly planned to provide the possibility to immediately preserve traffic data and other stored data worldwide





# Budapest Convention on Cybercrime

## 24/7 Contact Points

- Most contact points are police-based contact points
- Some are Prosecution Services contact points
- Budapest Convention provided a legal basis to the 24/7 network of contact points
- 24/7 networks are recognised as one of the most useful tools regarding international cooperation



# MLA request form templates



**Obtaining Assistance  
from the Hong Kong  
Special Administrative Region  
in Criminal Cases**

Guidelines for Making Application  
under the  
Mutual Legal Assistance  
in Criminal Matters Ordinance  
(Chapter 525, Laws of Hong Kong)

International Law Division  
Department of Justice  
Hong Kong Special Administrative Region

<http://www.doj.gov.hk/lawdoc/mla.pdf>

**Standard form of Request to Hong Kong SAR  
for Assistance in a Criminal Matter**

\*\*\*\*\*

**TO :** Secretary for Justice  
Hong Kong Special Administrative Region ("Hong Kong SAR")  
of the People's Republic of China

**FROM :** [name of appropriate authority/Central Authority of requesting place]<sup>2</sup>

**REQUEST FOR MUTUAL LEGAL ASSISTANCE  
IN A CRIMINAL MATTER**

**INTRODUCTION**

**EITHER :** I/The office of (name of designated authority under an operative bilateral agreement between Hong Kong SAR for mutual legal assistance), being the Central Authority designated (number of the relevant Article) of the Agreement for Mutual Legal Assistance between (name of requesting place) and Hong Kong SAR to make requests for mutual legal assistance in criminal matters on behalf of (name of requesting place), and being empowered by the relevant provisions of empowering legislation of requesting place to make requests for mutual legal assistance, present this request to the Central Authority of Hong Kong SAR.<sup>3</sup>

**OR :** I/The office of (describe appropriate authority, either person or office), being an authority by virtue of (state relevant provisions of empowering legislation of requesting place) to make requests for mutual legal assistance in criminal matters on behalf of (name of requesting place), present this request to the Secretary for Justice, Department of Justice, Hong Kong SAR.<sup>4</sup>

**REQUEST**

**EITHER :** This request is made under the Agreement between (name of requesting place) and Hong Kong SAR for Mutual Legal Assistance in Criminal Matters.<sup>5</sup>

**OR :** (Name of requesting place) makes this request for assistance to be extended to the Mutual Legal Assistance in Criminal Matters Ordinance, Chapter 525 of the Laws of Hong Kong.<sup>6</sup>

**MANDATORY ASSURANCES**

It is confirmed that this request :

- (a) does not relate to the prosecution or punishment of a person for a criminal offence that is, or is by reason of the circumstances in which it is alleged to have been committed or was committed, an offence of a political character;
- (b) is not made for the purposes of prosecuting, punishing or otherwise causing prejudice to a person on account of that person's race, religion, nationality or political opinions;
- (c) does not relate to the prosecution of a person for an offence in a case where the person has been convicted, acquitted or pardoned by a competent court or other authority of (name of requesting place), in respect of that offence or of another offence constituted by the same act or omission as that offence; and
- [(d) does not have as its primary purpose the assessment or collection of tax.]<sup>11</sup>

**ASSISTANCE REQUESTED**

The Department of Justice of Hong Kong SAR is requested to take such steps as are necessary to give effect to the following :

**1. Examination on oath/affirmation of a witness before a magistrate in court.**

(e.g.) Mr. X  
ABC Co., Ltd.  
(address)

to be orally examined on oath or affirmation on the following matters :

- (specify clearly relevant issues/areas relating to subject matter of criminal investigation/prosecution on which evidence of witness is sought and/or provide a list of relevant questions.)

**2. Production of things (documents, books etc.) before a magistrate, [and obtaining of oral evidence of the witness producing such material for the purpose of identifying and proving the material produced]<sup>12</sup>.**

(e.g.) Director  
ABC Co., Ltd.  
(address)

to be required to produce (describe form of evidence e.g. 'certified copies') of the following documents for the period (state relevant time frame) :

- (specify documents or classes thereof.)

<sup>11</sup> Necessary only if criminal matter is an investigation concerning offences relating to taxation and a bilateral agreement with Hong Kong SAR is in operation.

<sup>12</sup> Include this part if deemed necessary for purposes of admissibility of documents in evidence.

# [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/415038/MLA\\_Guidelines\\_2015.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415038/MLA_Guidelines_2015.pdf)




OFFICIAL

## Requests for Mutual Legal Assistance in Criminal Matters Guidelines for Authorities Outside of the United Kingdom - 2015

12<sup>th</sup> Edition

International Criminality Unit, Home Office, 3rd Floor Seacole Building, 2 Marsham Street, London  
SW1P 4NF

<b>SECTION 1: Introduction</b>	<b>4</b>
Role of Central Authorities in the UK	4
Requests for the Crown Dependencies and UK Overseas Territories	5
Types of Assistance	5
International Agreements	5
Reciprocity	6
Confidentiality	6
Collateral Use - Requests Made by the UK	6
Collateral Use - Requests Made to the UK	6
Law Enforcement (Police) Cooperation	7
<b>SECTION 2: How to Make a Request</b>	<b>8</b>
Is MLA Appropriate?	8
Who Can Send an MLA Request	8
De Minimis Requests	8
Dual Criminality	9
Language of Requests	9
Format of a Request	9
Transmission	11
Where to Send MLA Requests	11
Timescales	13
Queries about Requests	13
Urgent Requests	14
Cost of Executing Requests	14
Notification Where Assistance is No Longer Required	14
Linked Requests	14
Refusal of MLA Requests	15
<b>SECTION 3: Types of Assistance</b>	<b>16</b>
Service of Process	16
Statements and Interviews	18
Evidence on Oath/in Court	19
Hearings via Video or Telephone Conference	21
Asset Tracing	23
Production Orders	24
Search and Seizure	26
Communications Data	28
Live Interception of Communications	30
Restraint (Freezing)	31
EU Freezing Order	35
Confiscation & Forfeiture	36
EU Confiscation Order	39
Temporary Transfer of a Prisoner for Purposes of Investigation	40
Passport Information and Immigration Status	43
Transfer of Proceedings	44
Criminal Records	46
Judicial Records	47
Other Requests for MLA	50



# [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/415038/MLA\\_Guidelines\\_2015.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415038/MLA_Guidelines_2015.pdf)

## **MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS**

### **A GUIDE TO IRISH LAW AND PROCEDURES**

#### **Index**

##### Section

- |    |  |
|----|--|
| 1  | Introduction   |
| 2  | Central Authority for Mutual Assistance in Criminal Matters                  |
| 3  | Requests under International Conventions                                     |
| 4  | Authorities from which requests may be received                              |
| 5  | Form of requests, grounds for refusal and confidentiality (General)          |
| 6  | Scope of Irish law on Mutual Legal Assistance in Criminal Matters            |
| 7  | Information about financial transactions for criminal investigation purposes |
| 8  | Interception of telecommunications messages                                  |
| 9  | Freezing, Confiscation and Forfeiture of Property                            |
| 10 | Provision of Evidence  |
| 11 | Other Forms of Assistance  |
| 12 | Police to police enquiries   |
| 13 | Irish authorities empowered to make requests                                 |

#### **5. FORM OF REQUESTS, GROUNDS FOR REFUSAL AND CONFIDENTIALITY - GENERAL**

(1) Requests to be addressed to the Central Authority: Requests from designated states must be addressed to the Central Authority, unless the relevant international instrument provides otherwise.

##### Page

(2) Format of requests: Requests to the Central Authority for mutual legal assistance should be in writing or in any form capable of producing a written record under conditions allowing their authenticity to be established.

(3) Language of requests: All requests and any supporting documents should be in either Irish or English. In cases where requests are not in Irish or English, they must be accompanied by a translation into either of those languages and by a translation of any other such documents or the material parts of them.

(4) Requests to include the fullest information: In general, and subject to the requirements of Irish law set out in this guide and any requirements of the relevant international instrument, requests should contain the fullest information, in particular:

- (a) details of the authority making the request, including the name, telephone number and email address (where available) of a contact person
- (b) details of the purpose of the request
- (c) details of the person or persons named in the request including, where available, address, date of birth and nationality
- (d) a description of the offences charged or under investigation
- (e) a summary of the facts giving rise to the request
- (f) relevant dates e.g. date of court hearing (reason for special urgency or attention should be included in the covering letter of request)
- (g) a description of evidence sought, including, in the case of bank accounts, details of the relevant institution, account numbers and account names
- (h) specific information on any property to be searched and/or seized
- (i) details and supporting documents in relation to the freezing, confiscation or forfeiture of criminal assets

Ticket number of the previous request (if available): .....

DD/MM/YYYY



## URGENCY

### URGENT

Response expected by: DD/MM/YYYY

### REASONS FOR URGENCY

- ☐ Threat to life and limb    ☐ Offender in custody    ☐ Crime in progress    ☐ Volatility of data  
☐ Imminent threat of a serious nature to public security    ☐ The only evidence available  
☐ Statute of limitation due to expire    ☐ Other: \_\_\_\_\_

### DESCRIPTION/JUSTIFICATION FOR URGENCY

## CONFIDENTIALITY<sup>1</sup>

- ☐ The data submitted is only for request purpose  
☐ The data submitted can be used by the requested authority  
☐ The data submitted can be shared with other authorities

## OFFENCES SUBJECT TO CRIMINAL INVESTIGATION OR PROCEEDINGS

(Irrespective of their consideration in the requested State)

### OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND SYSTEMS / COMPUTER-RELATED OFFENCES

Choose an item.

### OFFENCES RELATED TO ORGANIZED CRIME AND CORRUPTION

Choose an item.

### OFFENCES AGAINST THE PERSON

Choose an item.

### OFFENCES OF FRAUD/FINANCIAL OFFENCES

Choose an item.

### OTHER SERIOUS OFFENCES

Choose an item.

### ANY OTHER OFFENCE (PLEASE SPECIFY)





## HOW IS THE DATA RELATED TO THE INVESTIGATION

## APPLICABLE LEGISLATION (SUBSTATIVE AND/OR PROCEDURAL)

Please cite the most relevant

Title of Legislation

Relevant Sections

Right to Request Data

Codes of Practice

Relevant Court Decisions

## CASE STATUS

☐ Pre-investigative phase   ☐ Investigate phase   ☐ Prosecution phase   ☐ On trial

Other details: .....

## DATA TO BE PRESERVED

☐ **Subscriber information** Please specify: .....

Period of interest Start date: DD/MM/YYYY End date: DD/MM/YYYY

☐ **Traffic data** Please specify: .....

Period of interest Start date: DD/MM/YYYY End date: DD/MM/YYYY

☐ **Content data** Please specify: .....

Period of interest Start date: DD/MM/YYYY End date: DD/MM/YYYY

## EXPECTED ANSWERS/RESULTS

- ☐ Confirmation for receiving the request   ☐ Confirmation for preservation of the data  
☐ Information of the amount of data preserved   ☐ Information of the type of data preserved  
☐ Information on the preservation period   ☐ Information on legal procedure used for preservation  
☐ Other: .....

## EXPEDITED DISCLOSURE OF PRESERVED TRAFFIC DATA (UNDER ART. 30)

Details/description of data<sup>2</sup>

## REQUESTING AUTHORITY DETAILS

Name

Address



Telephone number	
Cell phone number	
E-mail address	
Fax number	
Office Hours	
Time Zone	

**FOR VERIFICATION BY THE AUTHORISED PERSON, PLEASE CONTACT:**

Name:	
Job Title:	
Function:	
Signature:	

- ☐ Please let us know if, according to this information, you intend to build a criminal case within your country.
- ☐ Please let us know if you encounter issues taking into account this request.
- ☐ If the system is a shared system, please preserve all basic subscriber information for all virtual systems on the IP.

Ticket number of the previous request (if available): .....

DD/MM/YYYY

**URGENCY**☐ **URGENT**

Response expected by: DD/MM/YYYY

**REASONS FOR URGENCY**

- ☐ Threat to life and limb
- ☐ Offender in custody
- ☐ Crime in progress
- ☐ Imminent threat of a serious nature to public security
- ☐ The only evidence available
- ☐ Volatility of data
- ☐ Statute of limitation due to expire
- ☐ Other: .....

**DESCRIPTION/JUSTIFICATION FOR URGENCY**

**OFFENCES SUBJECT TO CRIMINAL INVESTIGATION OR PROCEEDINGS,**  
(Irrespective of their consideration in the requested State)

**OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND SYSTEMS / COMPUTER-RELATED OFFENCES**

<input type="checkbox"/>	Illegal Access
<input type="checkbox"/>	Illegal Interception
<input type="checkbox"/>	Data Interference
<input type="checkbox"/>	System Interference
<input type="checkbox"/>	Misuse of devices
<input type="checkbox"/>	Computer-related forgery
<input type="checkbox"/>	Computer-related fraud
<input type="checkbox"/>	Offences related to child pornography
<input type="checkbox"/>	Offences related to infringement of copyright and related rights

**OTHER OFFENCES SUBJECT TO CRIMINAL INVESTIGATION OR PROCEEDINGS**

<input type="checkbox"/>	Terrorism
<input type="checkbox"/>	Sabotage
<input type="checkbox"/>	Murder
<input type="checkbox"/>	Grievous bodily injury
<input type="checkbox"/>	Kidnapping, illegal restraint and hostage-taking



<input type="checkbox"/>	Racketeering and extortion
<input type="checkbox"/>	Rape/offences against sexual liberty
<input type="checkbox"/>	Sexual exploitation of children and child pornography
<input type="checkbox"/>	Trafficking in human beings
<input type="checkbox"/>	Illicit trade in human organs and tissue
<input type="checkbox"/>	Trafficking in stolen vehicles
<input type="checkbox"/>	Money laundering/Laundering of the proceeds of crime
<input type="checkbox"/>	Fraud
<input type="checkbox"/>	Counterfeiting currency
<input type="checkbox"/>	Forgery of means of payment
<input type="checkbox"/>	Forgery of documents
<input type="checkbox"/>	Counterfeiting and piracy of products
<input type="checkbox"/>	Bribery of national public officials
<input type="checkbox"/>	Bribery of foreign public officials and officials of public international organizations
<input type="checkbox"/>	Embezzlement, misappropriation or other diversion of property by a public official
<input type="checkbox"/>	Trading in influence
<input type="checkbox"/>	Abuse of functions
<input type="checkbox"/>	Illicit enrichment
<input type="checkbox"/>	Bribery in the private sector
<input type="checkbox"/>	Participation in a criminal organization
<input type="checkbox"/>	Organised or armed robbery
<input type="checkbox"/>	Illicit trafficking in narcotic drugs and psychotropic substances
<input type="checkbox"/>	Illicit trafficking in weapons, munitions and explosives
<input type="checkbox"/>	Illicit trafficking in cultural goods, including antiques and works of art
<input type="checkbox"/>	Illicit trafficking in hormonal substances and other growth promoters



#### APPLICABLE SUBSTANTIVE LEGISLATION

Title of Legislation	
Relevant Sections	
Right to Request Data	
Codes of Practice	
Relevant Court Decisions / Confirmation	

#### APPLICABLE PROCEDURAL LEGISLATION TO BE FOLLOWED IN THE OBTAINING OF EVIDENCE

Title of Legislation	
Relevant Sections	
Right to Request Data	
Codes of Practice	
Relevant Court Decisions / Confirmation	

#### CASE STATUS

☐ Pre-investigative phase    ☐ Investigate phase    ☐ Prosecution phase    ☐ On trial

Other details: .....

.....

#### ☐ SUBSCRIBER INFORMATION

##### Period of Interest

Start Date		End Date	
------------	--	----------	--

##### Data specification

<input type="checkbox"/> Subscriber names	
<input type="checkbox"/> User names	
<input type="checkbox"/> Screen names, or other identities	
<input type="checkbox"/> Mailing addresses	
<input type="checkbox"/> Residential addresses	
<input type="checkbox"/> Business addresses	

<input type="checkbox"/> Email addresses	
<input type="checkbox"/> Telephone numbers, other contact information	
<input type="checkbox"/> Billing records	
<input type="checkbox"/> Billing address	
<input type="checkbox"/> Payment method	
<input type="checkbox"/> Payment History	
<input type="checkbox"/> Billing period	
<input type="checkbox"/> Information about length of service and the types of services the subscriber(s) or customer(s) used	
<input type="checkbox"/> Any other identifying information, whether such records are in electronic or other form	
<input type="checkbox"/> Connection logs and records of user activity for the subscriber(s) identified above, including log-in history and records identifying sent and received communications	
<input type="checkbox"/> All communications stored in the account(s) of the subscriber(s) identified above	
<input type="checkbox"/> All files that are controlled by user accounts associated with the subscriber(s) identified above	
Name, username and postal address of the holder of the account	
Name, username and postal address of the holder of the account	
When was the account registered?	DD/MM/YYYY
Is the account still active?	

#### ☐ USER DATA

Service ID (Skype, Windows Live, Chat room, etc.)	
Social Networking Service ID (Facebook, etc.)	
IP address used for the initial registration of the account	
IP address used for the last registered access to the account	
IP address used for access to the account on <b>Date:</b> DD/MM/YYYY <b>Time:</b>	
IP address used for sending message from the account <b>Message details:</b> <b>Date:</b> DD/MM/YYYY <b>Time:</b>	
Other relevant data	





☐ **TRAFFIC DATA**

**Accessed IP address / range of IP addresses**

IPv4	1-255	1-255	1-255
Date		Time	
Time Zone			
IPv6 Address	Subnet – 64 bit	Host – 64 bit	
Date		Time	
Time Zone			

**E-mail Address Specification**

E-mail address		@	
Date		Time	
Zone Time			

**Person/Organisation details**

Business Name	
Legal Name	
Contact name	
Address	
Country	
Phone	
E-mail	

☐ **CONTENT DATA**

<input type="checkbox"/>	Electronically stored documents, records, images, graphics, recordings, spreadsheets, databases; calendars, system usage logs, contact manager information, telephone logs, internet usage files	
<input type="checkbox"/>	Deleted files, cache files, user information, and other	



<input type="checkbox"/>	data	
<input type="checkbox"/>	Archives, backup and disaster recovery tapes, discs, drives, cartridges, voicemail and other data	
<input type="checkbox"/>	All operating systems, software, applications, hardware, operating manuals, codes, keys and other support information	
<input type="checkbox"/>	Other:	
Origin of the data (if known)		
Destination of the data (if known)		
Other relevant details		

#### ACTIONS REQUESTED IN RELATION TO DATA

--

#### REQUESTING AUTHORITY DETAILS

Name	
Address	
Telephone number	
Cell phone number	
E-mail address	
Fax number	
Office Hours	
Time Zone	

#### FOR VERIFICATION BY THE AUTHORISED PERSON, PLEASE CONTACT:

Name:	
Job Title:	
Function:	
Signature:	



# What affects International Cooperation



# What affects International Cooperation



# **Bear in mind possible differences**

## **Legal System**

- ❖ **Common law**
- ❖ **Civil Law**
- ❖ **Hybrid**
- ❖ **Islamic law**

## **Different powers & functions same name**

- ❖ **Prosecutors/police**

## **Different codes of procedure**

- ❖ **Custody deadlines**
- ❖ **Powers to enter, search and seize**
- ❖ **Surveillance powers (technical & physical)**



# What affects International Cooperation?

Making requests:

- ❖ Legal Basis
- ❖ Domestic procedures  
(Bureaucracy/getting permission)
- ❖ Don't know who to contact
- ❖ Don't know how to make a request
- ❖ Don't know what can request
- ❖ Don't know how to write a request
- ❖ Lack of capacity and resources
- ❖ Politics
- ❖ Language



# What affects International Cooperation?

Receiving requests:

- ❖ Legal Basis
- ❖ Domestic procedures  
(Bureaucracy/getting permission)
- ❖ Lack of capacity and resources
- ❖ Politics
- ❖ Language



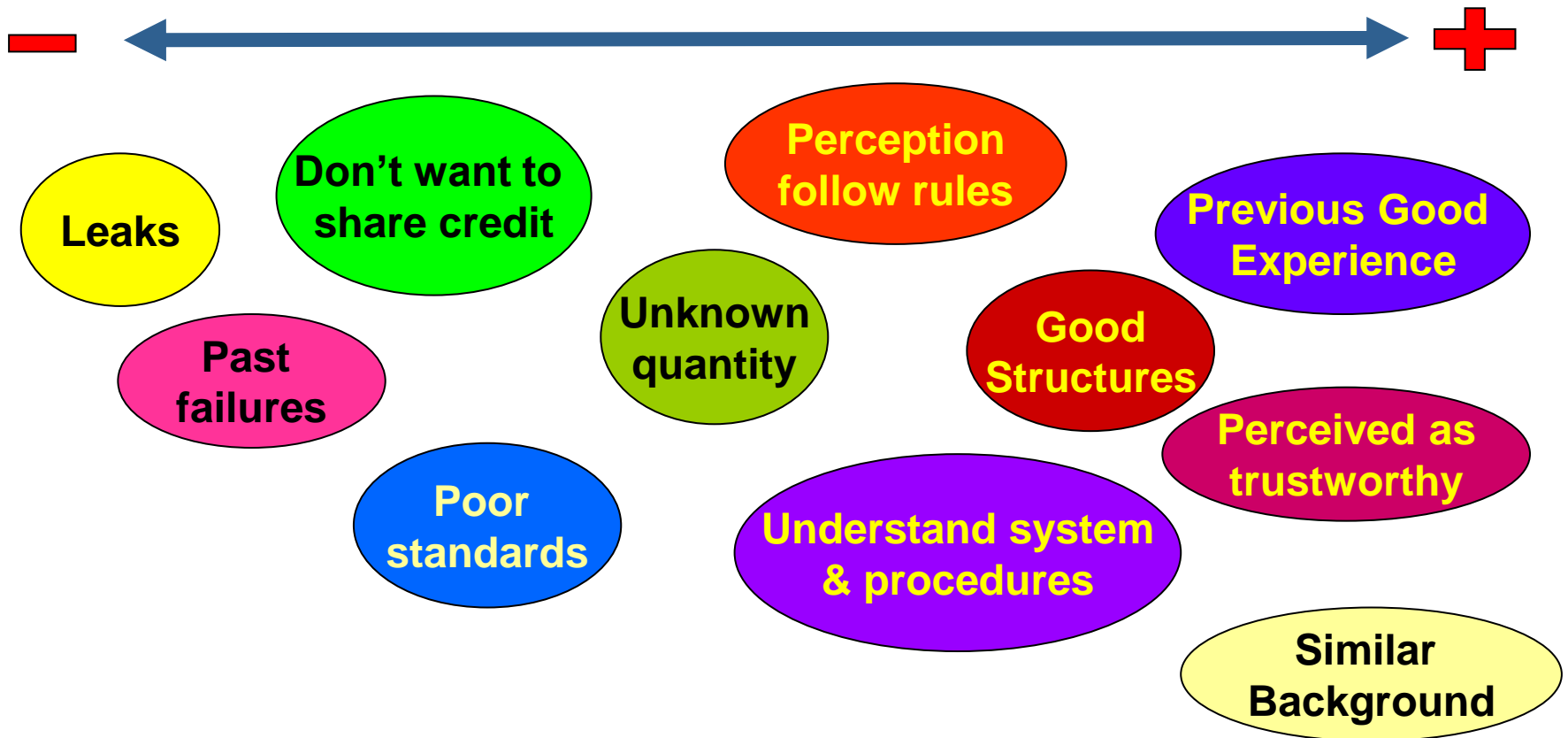


# What affects International Cooperation?

- ❖ Trust
- ❖ Capacity
- ❖ Skills
- ❖ Funding
- ❖ Culture
- ❖ Politics
- ❖ Legal Structure
- ❖ Speed
- ❖ Time
- ❖ Attribution



# Trust





# Capacity

- ❖ **Procedures exist to process a request**
- ❖ **Sufficient staff to process request**
- ❖ **Legally allowed to obtain evidence**
- ❖ **Appropriate forensic tools to process the data**
- ❖ **Appropriate equipment available (e.g. Faraday bags; secure storage)**



# Skills

- ❖ **Forensic specialists skilled in the area of investigation requested**
- ❖ **Specialist knowledge to request correct and appropriate analysis**
- ❖ **Know how to fill in the request to appropriate legal standard**
- ❖ **Competence in language of request**



# Funding

- ❖ **Forensic specialists remain properly trained and retained**
- ❖ **Able to purchase software licences**
- ❖ **Able to pay any 3rd party charges**
  - **ISP costs**
  - **Defence Attorney fees**
  - **Translation**
- ❖ **Able to pay for storage and secure transport of evidence**



# Culture

- ❖ **Is there a cooperation mindset?**
- ❖ **Has cooperation existed previously?**
- ❖ **Prepared to share the credit?**
- ❖ **Does hierarchy accept that impossible to go it alone?**



# Politics

- ❖ **Do the countries have a working relationship?**
- ❖ **Do those that authorise cooperation accept such a relationship is desirable?**
- ❖ **Are there other political issues that could work against cooperation?**



# Legal Structures

- ❖ **Is the dual criminality principle satisfied?**
- ❖ **Are the countries signatories to an appropriate legal instrument?**
- ❖ **Are the domestic laws and procedures in place?**
- ❖ **Do they work well enough?**



## **In final analysis, these are your aims:**

### **Electronic evidence inherent challenges:**

- ❖ **Identify and locate the evidence**
- ❖ **Secure the hardware**
- ❖ **Capture and analyse the data**
- ❖ **Maintain integrity and chain of custody**
- ❖ **Comply with rules of court and admissibility**
- ❖ **Link the suspect to use of the device at the relevant time ('Attribution')**

**International cooperation should support and facilitate them**





# Questions