Karim.Khan @ICC-CPI.int

Po Box: 19519, 2500 CM
The Hague, NL

Dear Karim Khan,

I have been interested in your work for a while and would like to request an open-hearted informal conversation about various security and compliance issues at ICC itself.

Note: This isn't a commercial offer, nor a trick to gain anything. It is merely an attempt to share specific knowledge to help ICC protect our safety and justice for all people.

Some background information:
****
****
*** mainly focused on structural ***prevention*** of espionage, sabotage and criminal infiltration.
While maintaining decent safeguard as core value to prevent corruption.

During a recent research project we noticed that there are some very serious security and law & regulations compliance issues with how ICC is handling information flows. This concerns me.

It not only means that ICC itself is partly operating outside the boundaries of various rules, regulation and international treaties, but also that subjects like espionage and intrusion-prevention seem to be a rather neglected concern within the present ICC structure.

Our main findings;
~ ICC is leaking quantities of sensitive and confidential inside_information to the public internet via various paths.

~ ICC leadership has 'allowed' 3rd party commercial companies to handle sensitive and classified ICC information, even companies with a rather dubious reputation like criminal convictions...
By doing so, ‘allowing’ espionage profiling of the organization, which people work for/with ICC and what operational activities are going on. While ‘tolerating’ unauthorized covert access to data handling systems.

~ ICC 'security' functionaries who are supposed to make sure that unauthorized access to ICC infrastructure and physical locations is not possible. Are seemingly sitting within a bureaucratic Ivory Tower composition whereby they “allow” indolent IT and operational security choices which are clearly not compliant with essential basic security guidelines and regulations.
Various simple protection measures are not even accomplished. Which is publicly visible.

Note: By partly neglecting the core task to actually “enforce” security rules and regulations on people who make key choices for the ICC structure. Those 'security' functionaries are allowing the ICC organization to be insufficiently protected. Therefor ICC is in breach of various regulations.

~ ICC 'security' functionaries do not seem to be “in control”, when it comes to preventing or detecting long term intrusion and extraction. As they are not “in control” of the data flows and accessibility.

There seems to be a lack of a complete overview diagram/picture of which data flows there are present.
So how can they be expected to even define which classification and protection maturity level all those forms and (sub-)layers of data/information ought to have ?

I’m concerned to see that the present security functionaries at ICC are partly neglecting to enforce all the essential mandatory “Security” rules on themselves, their fellow employees and service-providers.
After all, those 'security' functionaries currently do not get rewarded extra for making sure that ICC is decently protected and compliant. They do get paid for their work hours. So of course they appear to be making things look good on paper. As it’s better for their personal career when they don’t bother considerably with actually enforcing various rules and regulations...
Sensible rules which many within ICC can't be really bothered to adhere to, ..because they have not been made sufficiently aware of why it is of key importance to comply.
They even go as far as using various known (Machiavellian) tricks, like putting cunningly deceptive statements in official status reports to pretend that things are “okay” and compliant.
Even when it is publicly noticeable that things clearly are not “okay” at all.

Be that as it may, I would like to offer in-depth expertise so that you and your peers within ICC leadership can be better informed about what's going wrong with *risk management* and why.
More importantly, how you can simply make sure that protection and compliance is actually done properly.

Please feel free to send an invitation, so that we may exchange key knowledge on location in Den-Haag.

Met vriendelijke groet | With kind regards | Med vennlig hilsen
* *******

eMail: **********
Tel: +31.6.********

International Criminal Court

Trying individuals for genocide, war crimes, crimes against humanity, and aggression

Administration of Justice · The Hague, Zuid-Holland · 231K followers · 501-1K employees

Home | About | Posts | Jobs | People

1,531 associated members

Search employees by title, keyword or school

What they do

685 | Legal
215 | Administrative
214 | Business Development
166 | Operations
160 | Education
125 | Community and Social Services
117 | Information Technology

Where they live

749 | Netherlands
688 | The Randstad, Netherlands
650 | South Holland, Netherlands
623 | Rotterdam and The Hague
557 | The Hague
132 | India
84 | United States

Where they studied

93 | Leiden University
30 | University of Amsterdam
28 | University of Paris I: Panthéon-Sorbo...
24 | Paris-Pantheon-Assas University
21 | University of Oxford
20 | Utrecht University
20 | University of Cambridge

What they studied + Add

356 | Law
241 | International/Global Studies
210 | American/U.S. Law/Legal Studies/Ju...
199 | International Law and Legal Studies
108 | Criminal Justice/Safety Studies
86 | Human Rights
85 | Political Science and Government

Adrian Agius · 3rd
Legal Technology @ International Criminal Court
2K followers
Follow

Saleh Mansour · 3rd
Criminal Intelligence Officer
3K followers
Follow

David Hasman · 3rd
Head of eDiscovery and Data Analysis
Connect

Karim E. · 3rd
Protection and Risk Management Officer at
Connect

Carlos Anast... · 3rd
Security Advisor in an International Organization

Wilhelmina W... · 3rd
Investigator, Independent oversight mechanism (ICC)

Geofrey Lugu... · 3rd
Security, Safety and Risk Management Professional

Corporate Security & Public Administration Specialist

[redacted] · 3rd
[redacted]
[redacted] followers

Gocha Lordki... · 3rd
Judge, International Criminal Court
500+ connections

Pavle Nozadze · 3rd
Data Management Officer at International Criminal Court

Michel Schindeler · 3rd
Security officer bij International Criminal Court
Amsterdam. Contact info 500+ connections
Marcel Wilschut
Security Officer

Nazhat Shameem Khan · 3rd
Deputy Prosecutor International Criminal Court
Netherlands · Contact info
[redacted] connections

International Criminal Court
University of Cambridge

Connect | Message | More

About

A lawyer by profession, and a former judge of the High Court of Fiji, Nazhat Shameem was Fiji's Permanent Representative to the United Nations in Geneva, Switzerland until the 28th of February 2022. She was also Ambassador to Switzerland. On the 15th of January 2021 she was elected President of the UN Human Rights Council in Geneva, for 2021. In December 2021 she was elected a Deputy Prosecutor at the Office of the Prosecutor at the International Criminal Court at The Hague in the Netherlands for a term of 9 years.

Security Officer
International Criminal Court · Full-time
Oct 2016 – Present · 7 yrs 8 mos
Den Haag en omgeving, Nederland

- Provide a professional protection force securing the seat of the Court.
- Control access and egress to ICC premises in accordance with approved policies.
- Ensure the safe custody of all detained persons whilst at Court or elsewhere within th
- Operate the ICC Security Control Centre, including monitoring of an extensive CCTV, communications, fire prevention and alarm systems surveillance system.
- Secure and escort VIP's, sensitive witnesses and other personnel whilst in the premis
- Provide an emergency response capability within the ICC premises.
- Maintain all necessary records to ensure the effective functioning of the Section.
- Submit detailed investigation reports on security related incidents.
- Complete and pass all specified induction, refresher and other specialist training.
- Any other ad hoc duties as assigned by the Chief of Security.

Beveiliging

Politieagent
Politie Nederland · Full-time

etc...

A few more thoughts for contemplation:

~ Who decided that it's a “good” idea, to ‘allow’ various forms of cyber-attacks and espionage, by neglecting to implement several basic tactical defence machanisms ?
Why is ICC not simply preventing vulnerability profiling probes and weakest link scans, to prevent hostile actors from even locating various shortcomings/mistakes/gaps/back-doors/etc...

~ Who decided that it's a good idea, to let IT and various external service providers choose problematic products which are notoriously known for their endless security issues (CVE's), due to subversive conflict of interest? It seems as though some dubious products are chosen anyway because of intriguing ties with those who ruthlessly sell those substandard products & services for their own financial gain.
Even products which regulate who gains (remote) access. **Example:** login.icc-cpi.int/logon/LogonPoint/tmindex.html
There is no need to lower the protection level by letting IT people choose dubious service products.
It is rather odd, especially when there are plenty of options to choose from which are actually proven to be “Secure by Design”; user-friendly; low maintenance; low cost or free for use.

~ Who decided that it is a good idea to allow internal confidential 'meta-data' to travel outside physical buildings into the public domain? Thus, also giving it to hostile actors and espionage organizations.
* 'hidden' meta-data information in files, documents, emails, communication-services-protocols, ..etc...

~ Who decided that it's a good idea to allow ICC security functionaries to publish information to the internet about themselves and their roles and the organization, and so on..
By doing so, undermining the security structure of not only ICC but also organization which ICC deals with.
By publishing all those details without the “need” to do so, they make themselves and the organization extra vulnerable for**:** Bribes & Blackmail; Profiling; Targeted attacks; hacking via personal devices (APT's, etc); Data breaches; Social Engineering; ..etc... ; ..etc..
Thus creating many security problems as ‘security functionaries’ themselves.
In my opinion, security functionaries should **not** publish about who they are and what is going on.
They ought to respect the age-old basic tactical safeguard rule: “Need to know”.

“Sed Quis Custodiet Ipsos Custodes”