CISE and the "Responsibility to Share" principle

Fernando del Pozo

Director, Wise Pens International

Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001 by the US House and Senate Committees on Intelligence

"9. Finding: […] agencies did not adequately share relevant counterterrorism information […] This breakdown of communications was the result of […] differences in the agencies' missions, legal authorities and cultures. Information was not sufficiently shared, not only between different Intelligence Community agencies, but also within individual agencies, and between the Intelligence and the Law Enforcement Agencies."

(Notice that it doesn't say that there was not enough information, just that it was not shared)

In more detail:

- Prior to 11 Sep 2001, CIA and other intelligence agencies had credible rumours that AQ was preparing a terrorist attack using commercial aircraft as a weapon
- US Customs was aware that several Saudis, potential AQ operatives, had irregularly obtained 6 months stay visas and entered the US as tourists/business and students
- Meanwhile, the FBI learned that a group of Arabs were taking flight lessons, in particular on “executing turns and approaches” but that they were strangely uninterested in the take-off and landing parts of the course

… but no one was able to put together these pieces of information, which would have permitted to abort the attack, because under the “need to know” rule they had no access to the other info strands

The 11 Sep 2001 case was well documented and made public* but according to the media there are strong indications that, at least, the failures to prevent the attacks in Paris on November 2015, and Barcelona on August 2017 had the origin in similar "*breakdown of communications"* between LEAs and intelligence communities.

* The report was originally top secret, but eventually downgraded to non-classified

… in other words:

The “need-to-know” (NTK) rule governed (and still governs today in Europe) the diffusion of information between intelligence and LEAs. This principle requires, for the information to flow, a positive answer to two questions posed and answered by the “owner” of the information:

- Does the potential addressee need to know it?
- Is the potential addressee in possession of the necessary credentials?

The problems of “Need-to-Know”

- The party which has come about a certain piece of information becomes the “owner”, empowered to decide about its diffusion (instead of a contributor to the collective task of building intelligence out of several pieces of information). This is irrespective of this party’s position in the hierarchy.
- The party in need of a piece of information which is in other party’s possession does not even know that it exists, hence cannot request it.
- Questions to the community (“*does anyone know something about this*?”) are never successful.

The result:

- Intelligence and LEAs become watertight compartments

This does not imply that info protection is not important, as, understandably, excessive diffusion can be counterproductive. However, NTK nearly always errs on the side of restriction.

Enter the new paradigm: "Responsibility to Share" (RTS)

Definition: *An individual in possession of a piece of information is responsible for disseminating it to anyone that may have a legitimate use for it, and would be accountable if any harm happens as a consequence of the non-distribution.*

It is enshrined in two of the CISE principles:

2. CISE must increase maritime awareness based on the **responsibility-to-share** principle.

10. CISE subscribers and stakeholders are entitled to obtain information only if they also contribute in a way commensurate with their capabilities.

Formal bases for RTS

- Principle of Solidarity, TFE Art 222: “the EU and MSs shall act jointly in a spirit of solidarity if a MS is the object of a terrorist attack…” (*this includes not only reaction, but also* ***prevention***)
- UNCLOS, Art 24: “[T]he coastal State shall **give appropriate publicity** to any danger to navigation, of which it has knowledge, within its territorial sea”
- UNCLOS, Art 200: “States shall cooperate […] encouraging the **exchange of information** and data acquired about pollution of the marine environment”
- SUA Convention, Art 13: “1. States Parties shall co-operate in the **prevention** of the offences set forth in Art 3 (*piracy, terrorism or other violence against ships*) particularly by: […] b) **Exchanging information** in accordance with their national law, and […] other measures taken as appropriate to prevent the commission of offences set forth in Art 3.”

Restrictions/limits to RTS

Caveats based on national security and sovereignty:

- SUA Convention: *"[…] in accordance with their national law*"
- UNCLOS, Art 302: "*[…] nothing in this Convention shall be deemed to require a State Party […] to supply information the disclosure of which is contrary to the essential interests of its security"*

However:

- Common EU membership, and actors being LEA or other Government agencies, should alleviate the rigour of these restrictions

Other, less generic, restrictions:

- Judicial secret. This is obviously a hard restriction, but not frequent
- Commercial confidentiality (e.g., shipowners' legitimate desire to hide activities from competitors) → *This concern should also be alleviated by considering that the actors are LEA, hence not commercial competitors*
- Contractual obligations (e.g., satellite company selling imagery on condition of non-distribution to third parties) → *This could be solved by amended contracts*

How to implement RTS?

- NTK is based on "***do not*** *share unless…*"
- RTS is based on "*share unless…*"

Problem:

- Positive guidelines are harder to encode and enforce than prohibitions (compare "do not cross on red light" with "cross on green light": the first is an absolute rule for pedestrians, the last depends on other factors which must be specified, e.g., a desire or need to cross)

Hence, RTS is harder than NTK to:

- Encode: During EUCISE2020 WPI has drafted a detailed list of guidelines (but we feel they still need polishing)
- Enforce (the real core of the problem): next slide →

How to **enforce** RTS?

Is RTS a "*moral obligation*"? A "*soft law*"? (both have been proposed)

IMHO both descriptions result in RTS appearing less exigent than it must be, and therefore reduce the agencies' willingness to abide wholeheartedly by RTS

Solution:

Reinforce the participants' awareness of the importance of RTS by:

- Publishing statistics of *push* and *pull*
- Conduct RTS audits (which must absolutely include personal interviews IOT evaluate the commitment: this is not a purely technical matter)

10. CISE subscribers and stakeholders are entitled to obtain information only if they also contribute in a way commensurate with their capabilities.

All this will have to be solved during the transitional phase if we want CISE to be the instrument that we need to fight terrorists, pirates, traffickers and other criminals operating at sea, but especially if we want to get ahead of their sinister plans.

And it will take time, it is not easy to go against the weight of corporate traditions and established operating procedures.

The big prize: CISE, if successful in implementing the **Responsibility to Share** principle for maritime security, may become a model for other non-maritime law enforcing environments, at least in Europe, if not beyond.

We must not allow a breakdown of communications to be again the cause of such catastrophic failures as those mentioned before!

Bottomline:
Common Information-Sharing Environment
and its **Responsibility to Share** principle,
(if implemented unreservedly)
will be a bellwether in building trust among
the MSs Intelligence and Law Enforcing
Agencies, which will strengthen overall
cohesion in the European Union


Thanks

The “Responsibility to Share” principle

Fernando del Pozo

Director, Wise Pens International