INTERPOL

# Statement

by

Jürgen Stock

# UNITED NATIONS SECURITY COUNCIL OPEN DEBATE ON THE PROTECTION OF CRITICAL INFRASTRUCTURE AGAINST TERRORIST ATTACKS

13 FEBRUARY 2017

VIA VIDEOCONFERENCE FROM LYON, FRANCE

Mr. President,

Your Excellencies,

Ladies and Gentlemen,

It is an honour to brief the Security Council once again, and on an issue of central importance to our collective security.

I would like to thank Ukraine for convening this meeting, and their continued efforts to mobilise international cooperation on this crucial subject.

Critical infrastructure acts as the life support system of our everyday existence. Our societies are sustained by a highly complex and sophisticated network of infrastructure systems. Our citizens expect

and rely upon functioning institutions and services for their health, safety, security, and economic well-being.

This life support system has become more efficient and productive due to technological advances, the interchanges of globalisation, and the demands of an increasingly urban population. The advent of *life 3.0* - the overlapping of the digital and physical world – allowed us to monitor and even control infrastructure from anywhere in the world.

However, with heavy reliance and real-time connectivity comes vulnerability to threats. The interdependence of our infrastructure through sectors and industries, between cyber and physical areas, and across national boundaries, means that the consequences of an attack could be far-reaching.

One attack on a single point of failure could lead to the disruption or destruction of multiple vital systems in the country directly affected, and a ripple effect worldwide. This creates an appealing target to

those intending to harm us. And as our cities and infrastructure evolve, so do their weapons.

Conflict zone tactics - such as simultaneous active shooter events; armoured vehicle-borne improvised explosive devices (VBIED); home-made explosive vests; hacking attacks; or portable Unmanned Aerial Systems with explosive payloads – could be honed for use in our city streets and against key facilities.

So how can we protect the vital organs of our life support system against this ever-adapting threat?

The short answer: by getting all relevant actors able to prepare; prevent; and respond to such attacks. These imperatives are at the core of INTERPOL's efforts – along with our partners in the CTITF Working Group - to promote intelligence sharing, capacity building and resilience in some crucial areas.

First, we focus on strengthening critical site security with emergency preparedness standards and procedures.

- For instance, INTERPOL's Vulnerable Targets team has been working with our member countries in West Africa to enhance the physical security of laboratories hosting dangerous pathogens and protect them from terrorist attacks. Generously funded by the Canadian government, this project seeks to build biosecurity action plans through joint inter-agency action.

Second, we continue to urge countries to protect their borders and counter terrorist mobility.

- As mentioned in the UN Secretary-General's report on the threat posed by ISIL, discussed here last week: between October 2016 and January 2017, INTERPOL observed a 63 per cent increase in the number of

profiles of foreign terrorist fighters accessible in real time through its criminal information system and a 750 per cent increase in the sharing of information by member countries through its channels. This is simply unprecedented in such a sensitive area – the call issued by the Security Council created a watershed.

Third, it is essential to remain vigilant and increase efforts to interdict materials and tools before they become the next weapon.

- In this context, INTERPOL works closely with the IAEA on mitigating the illicit trafficking of radiological and nuclear materials, through training in monitoring and detection, and cross-border operations.

Lastly, and above all, INTERPOL encourages inter-agency and international collaboration, as a force multiplier. The exchange of information, urgent threats detected, and best practices on

identifying vulnerabilities, methodologies, and lessons learned is crucial.

In law enforcement, we are keenly aware of the tragic paradox: a terrorist incident is often among the best opportunity for learning and improving. Sharing these lessons across borders means reaping the benefits, without paying that cost. It's a win-win scenario.

Together, we can build a global infrastructure security toolkit, and incident response mechanisms based on real-life operational experience. In parallel, we can test ourselves with plausible scenarios we may have to face in the future.

- To this end, INTERPOL organises events for experts from all involved stakeholders. Our joint symposium hosted with the US FBI is a case in point. Our recent Digital Security Challenge, together with private sector specialists, is another example of how we are working

with member countries and donors to prepare, prevent and respond to threats – be they physical, digital, or both.

Mr. President; Your Excellencies,

In an interconnected world, we will not succeed in protecting national infrastructure in isolation. This is why initiatives such as this meeting - and the steps that will be taken as a result by the international community - are essential.

Thank you for your attention.