VIENNA REMARKS FOR THE CONFERENCE ON THE HUMANITARIAN IMPACT OF NUCLEAR WARFARE

I would like to start these remarks by thanking the organizers of the conference for having me here in Vienna – it is an honor to be here and I am grateful for the opportunity to contribute to this important conversation.

I am Camille François, I am a Fellow at the Harvard Berkman Center for Internet and Society and a consultant on matters relating to cyberspace policy. My research and work addresses cyberpeace: the building of structural mechanisms to prevent conflict escalation in cyberspace and to ensure freedom, trust and security online.

These short remarks today address the intersection of cyber warfare and nuclear warfare, and the reasons why the current developments of cyber warfare pose great concern for nuclear safety. In three quick points, it relates to the vulnerability of nuclear assets to cyber operations, to the difficulties in securing them, and to evolution of both norms and state practice in the cyber realm.

First point - Nuclear assets are particularly vulnerable to cyber attacks, and this for at least two obvious reasons:

▪ They are complex systems heavily computerized.
Cf. Eric Schlosser's remarks: the complexity of these systems creates many points of vulnerability, attack surface is wide, many contractors operate in this environment. Cyber weapons targeting nuclear assets can therefore take advantage of the numerous vulnerabilities of these "complex machines", create great damage and conceal their traces while tricking systems into believing nothing unusual is underway.

▪ Nuclear assets remain prime strategic targets
Cf. Stuxnet. A public confirmation in 2010 that cyber weaponry could cause tangible offline damage – "break things". Designed to target and sabotage the industrial programmable logic controllers of the centrifuges of the

uranium enrichment facility at Natanz in Iran. State-developed.

Second point - Nuclear assets are particularly difficult to secure

Stuxnet lesson: main actors interested in cyber operations against nuclear assets are States with well-funded cyber weapons development capabilities.

When addressing the overlap of cyber and nuclear, hard not to think about the 1983 movie "War Games" in which a kid whose prime interest in hacking is changing his grades on the school computer network inadvertently penetrates a U.S. military network controlling the nuclear arsenal and triggers a great nuclear scare and an escalation scenario that would lead to the third world war. The movie does a good job at capturing a perception of the cyber / nuclear overlap risks in the 80's and is credited with impacting U.S. cyber policy at the time - President Reagan - who had close ties to Hollywood - had a private screening at Camp David. Generated harsh anti-hacking laws to prevent kids from fooling around in others' networks, and a belief that ensuring operational control systems couldn't be accessed from the Internet would address the key risks.

How can nuclear assets be vulnerable to cyber attacks if they are completely disconnected from the Internet? is a question answered in theory by many cyber experts looking at ways to "jump the air gap", and in practice by Stuxnet (again). In that case, infection by flash drive targeting contractors of the plant.

▪ Leads us to second point, which is: the main threats here are not coming from kids who want to change their grades, but from State actors who are heavily investing in cyber weaponry and who are seeing it as a new battlefield - "the fifth domain of war". + fears that terrorist groups would ne day develop such capabilities, notably by reusing and studying code from cyberweapons developed by States.

Third point - Cyber weaponry and offensive cyber operations are growing unchecked.

Some nations around the world are heavily investing in cyber weaponry. Exact growth of cyber offensive operations investment is hard to monitor for obvious secrecy reasons + one of the key characteristic of cyber is blurred line between defense and offense, so hard to establish how much funds are dedicated to growing a cyber arsenal as States increase their budgets for cyber defense. Could take the U.S. example - here from Shane Harris "@War" Book - U.S. DoD plans to spend 26 billion dollars on technology for cyber offense & defense over the next five years. That of course triggers over States to build their arsenal, both in defense and offense – which is why people worry about "cyber arms race".

Creates concern for two reasons:

▪ <u>There is something about the nature of cyber weaponry that is particularly worrisome: it spreads</u>. When cyber weapons targeting nuclear assets are designed and deployed, chances are high that they will spread to other assets – which is how the Stuxnet worm was discovered by a cybersecurity research firm. In reality, cyber weapons are therefore quite unpredictable. Also, this increases chances that the know-how spreads. Many elements can be necessary to conduct a cyber operation – like zero day vulnerabilities, special ops, etc. – yet ultimately the cyber weapon is code, lines of code that malicious actors can study and learn from when it replicates itself on other machines they might get access to. Also something we saw after Stuxnet – the reusing of the code in other malware. States' new playing field is also a training ground for other malicious actors.

▪ Second reason is that the <u>rules of the road for States to engage in cyber operations are very unclear</u>. Many States have declared that International Humanitarian Law applies to cyber operation, yet there is no consensus on how exactly it does. Cyber domain is a domain in which we dramatically lack mechanisms and norms to avoid conflict escalation. Easiest domain to circumvent other norms that are crafted to create peace and stability – like in the nuclear realm.

Maintaining peace in a nuclear world and securing complex nuclear systems is hard enough a mission – no need to add an intersecting layer of unchartered and dangerous conflict mechanisms. This is why the stakes of cyber peace extend way beyond cyberspace, and why we must build it together.

I thank you again for having me with you in Vienna for this important discussion.