FIRST Address to the Global Commission on the Stability of Cyberspace
Marina Bay Sands, Singapore, September 19th, 2018

Esteemed Commissioners, dear invited guests,

My name is Maarten Van Horenbeeck, I am a Board member of the Forum of Incident Response and Security Teams (FIRST). We are an association of 438 cybersecurity teams in government, private sector and academia from 90 countries. Our members are often referred to as the “fire brigade” of the internet and are the first ones to respond to major cybersecurity incidents.

Our goal is to make Computer Security Incident Response Teams, or CSIRT, more effective. We do this in four ways:

1. Ensuring a wealth of capable and competent incident response teams exist that are ready to respond to complex incidents, through training and education;
2. Building a community where CSIRT can easily find other trusted incident responders that have specific skills, such as product security teams, or proximity to an affected network, system or user. We do this by expanding our membership base, and through our Fellowship program;
3. Ensuring CSIRT have a common set of tools, including technological standards, they can use to more effectively respond to an incident;
4. Educate third party stakeholders, such as policymakers, on the work of our member teams, and how they can help address our ongoing needs and challenges.

FIRST deeply values the work of the Global Commission on the Stability of Cyberspace, and applaud and support your efforts to promote mutual understanding between the various communities operating the internet.

As you embark on your discussions here in Singapore, there are some specific challenges I would like to bring to your attention from our community, that we recommend considering:

- First, there has been a major increase in the number of incident response teams with national responsibility being initiated. However, the **mere existence of a team does not guarantee its effectiveness**. Incident Response teams run on trust. Trust is the sensitive outcome of a process that takes into account the needs of a wide diversity of stakeholders. While top-down implementations can meet these requirements, they often do not. FIRST invested significantly into assessing these needs and challenges as part of our contribution to the IGF’s Best Practices Forum on CSIRT in 2014. We encourage everyone to review the paper this forum published. It documents the challenges involved in building trust and contains a number of specific recommendations. In our view, continuing to increase the level of trust in our community is an important requirement for

building a stable platform for cooperation.

- Second, in recent years, we have seen the **inclusiveness of the defensive cyber security community be affected by worsening relationships between states**, including due to sanctions. While offensive state behavior on cyberspace increasingly affects internet users in various negative ways, the dominant threat to a user's everyday use of the internet is not a state. We believe limited exceptions should be carved out in sanctions regimes to enable defenders to effectively cooperate across boundaries. This conversation should take into account the obvious, but limited, risks defensive information sharing has in enabling offensive behaviors.

- Third, FIRST is excited to see the development of norms that support the development of trust, understanding and appropriate "rules of the road" for behavior in cyberspace. We encourage the Commission, and other organizations developing these norms, to focus on two very specific elements of norms development. These areas are the **inclusiveness of the development process**, and **norms implementation**.
    - Regarding **inclusiveness**, the IGF's Best Practices Forum on Cybersecurity is focusing this year on taking a multi-stakeholder look at cyber norms. From this effort, it is clear that there is a wide variety of norms development forums, but few take a multi-stakeholder approach to the issue, and keep an open mind on the definition of a "social norm" in cyberspace. A variety of more technical, or civil society inspired norms have appeared, such as the *Manila Principles*, or the *Mutual Agreed upon Norms for Routing Security*. These are not often considered or discussed in the same forums as state-proposed norms. We're excited that the GCSC itself is a multistakeholder body, and applaud your work.
    - In terms of **norms implementation**, due to the wide and uncoordinated development of cyber norms, we see a risk that norms are being proposed which do not gain widespread support. We strongly encourage participants in this community to find creative ways to support and back norms implementation through hard funding. For instance, economic incentives can be created for states to protect the "core of the internet" by encouraging them to invest in efforts to harden critical software components. This discourages the investment in offensive technology against the core by making it more expensive and challenging. It will also discourage its widespread use.

With this, I thank you again for your work, and we look forward to contributing to the important work of this commission in any way we can be of support. Thank you for the opportunity to deliver this address, and I wish you a productive meeting.

Maarten Van Horenbeeck
Board Member, Forum of Incident Response and Security Teams