Fr	B	C	NY	S	T	Total
2	7	7	10	7	10	

Example:
Berlin: an unprecedented collaborative effort between Fraunhofer Institutes active in the field of networked security systems for situational awareness and crisis management on one side and some crucial technology system providers on the other has enabled the first responder and security communities of Berlin to have an innovative demonstration scenario at their disposal starting in August 2013. It will provide all relevant stakeholders with a unified platform to connect and integrate different pieces of information in order to generate a comprehensive set of data/images which is crucial for an efficient and effective management of security processes and decisions in very complex environments.

1. Differentiated description of the key field

The "smart city" concept has been well established among the applied research communities focusing on urban systems. The key premise of this concept is that any urban infrastructure, both physical and social, will increasingly be interconnected, hence depended on and crucially important for numerous other sectors of the urban system. Hence, this drive should result in a higher quality of life and other amenities for citizens whilst contributing to a more efficient and effective use of resources, time, distances, processes and so on. However, so far this concept has mainly been driven by communities looking at the very structure, efficiency and optimization of such networks. With respect to urban security and resilience, the "smart city" concept will increasingly allow security relevant players to share and utilize important data of infrastructures and processes in a city for both better preparing the city for scenarios that will likely occur. At the same time, once a disaster has hit, a smart networked security community is much better capable of mitigating the consequences of such events and more safely and effectively coordinate all emergency response operations. On top of that, the connection of data sets stemming from different sources also offers cities a tool to better understand and, in turn more successfully tackle systemic risks and vulnerabilities at an early stage before they even get to the point of manifestation. Evidently, the latter encompasses threats and risks that may result from malicious intent (crime, terrorism, organized crime, trafficking) as well as from the power of nature (storms, floods, etc.).
However, the smarter urban systems get and the more connected they are, the more their vulnerability towards manipulation, malfunction as well as systemic collapse is likely to increase. Consequently, smart urban systems can only be 'really smart', if each link and node (i.e. buildings, power stations, traffic and logistic networks, etc.) of the complex network is intrinsically secure. Then, networked security solutions have a huge potential to support urban security communities to better prepare for and react to any challenge resulting from naturally caused or man-made disaster.

2. Reference to sustainability:

The link between sustainable urban development and networked security solutions is striking. A well organized and efficiently managed connection of security relevant data from various urban sectors allows enables a city government to increase its long-term all-hazard resilience on various levels:
First, comprehensive situational awareness spanning across all so-called critical infrastructure sectors can only be achieved via systematically linking relevant data, analyzing correlations and dependencies in order to identify possible short comings, inefficiencies as well as the aforementioned systemic risks. As a result, a city will be much better able to plan for specific crisis scenarios. It will be able to design and connect critical functions of the urban system in a way that they can better cope with future challenges.

Second, once a crime has been committed, an accident has triggered a blackout in an urban district or a fire has severely damaged a power station, only a well-informed responder community (police, fire fighters, technical relief forces, etc.) can swiftly respond to and help recover from such an incident.

Third, from an economic standpoint, the infrastructural damages and the economic losses that may cascade from one urban system to the next can be enormous. Thus, networked security solutions of tomorrow ought to be capable of detecting and identifying possible threats at a very early stage in order to limit such economic damages.

At last, the very latest debates among especially the intelligence communities on the misuse and manipulation of large masses of data within the entire realm of public and private (corporate) data points to a social risk and challenge of this topic: Especially ethical issues and privacy protection play a crucial role when introducing new technological applications for networked security concepts, which in the end may determine the acceptance of the urban population of such solutions. Not comprehensively considering the latter when designing and communicating the functioning of such systems to the broader public poses a serious threat for their successful implementation.

3. Relevance to industrial sectors?

Mobility:	High
Energy:	High
Production & logistics:	High
Security:	High
ICT:	High
Water infrastructure:	Middle
Buildings:	High
Governance:	Middle

Brief description of the high level of importance:
Just naming some buzzwords such as ‚smart grids', ‚autonomous and fully electric mobility systems', ‚fully automated logistic processes' underscore the fact that all of the aforementioned opportunities as well as risks related to utilizing data from these sectors for security relevant operations must be highly prioritized by the relevant sectors. Tracking a vehicle or a parcel within a large city, managing a serveral-hour blackout in a quarter or having a major public legal data networked hacked, all underscore the criticality of this topic.

4. Impact (positive & negative)

Positive:
- Early detection of risks and systemic vulnerabilities is much easier
- Interdependencies of different networks can be more easily monitored
- Impact of incidents can be much better calculated, hence facilitating a much improved risk-management
- Search and rescure operations can be conducted more efficiently
- In the aftermath of an incident all involved security forces can act and operate more effectively and efficiently
- Redundant resources to monitor same security issues can be saved

Negative:
- False conclusions or correlations between various data sets and sources can have severe impact on public acceptance of such systems
- Data protection and privacy issues have to be actively addressed
- Ways and means for the intrusion or manipulation of such systems must be well known and ideally eliminated

5. Implementation measures:

As the example of Berlin has shown, a well functioning networked security solution can only be realized if all relevant stakeholders (for example owner and operator of infrastructure + police + city administration + technolgoy provider + research and academia) share a common interest and find an agreement of the sensitive issues already mentioned. Thus, in order to advance the successful application of such systems, legal frameworks are most likely the key to a successful deployment, especially in the Western hemisphere. On top of that, the overall IT-architecture of such systems and their ownership is another such key success factor. Even more so when it comes to propriety issues among the public and the corporate world.

6. Actors: Who can shape things?

As already stated, the first step to more system integration, data sharing and monitoring lies within the regulatory bodies of a city, to be more precise in most democratic states it lies within the prerogative of national policy making. Hence, governments first of all have to create a legal framework that paves the way for a large-scale application of such systems. Second the large technology providers in close cooperation with the city officials responsible for data integration and security processes have to jointly define an architecture for a flexible integration of various sub-systems of the city. At last, owners and operators of the various urban infrastructures have to have the willingness to provide the city with relevant access to data and ICT-processes in order to make to overall system work.

7. Prerequisites:

Adjustment of legal frameworks
System architecture has to provide an operator interface for additional components and sub-systems to be integrated

8. Obstacles/barriers:

- Data protection and privacy rights
- Poor PR-incidents (e.g. NSA scandal)
- Missing interfaces
- Public anxiety ("big brother is watching – syndrome")

9. Indicators:

First and foremost, it would be helpful to have an overview on the entire set of data that security relevant players in a city have access to. Evidently, this is completely different depending on the cultural and legal background of the respective city. But once that picture could be generated – which as of today is hardly feasibly and could only be achieved via a comprehensive anaylsis of the security law of the various countries – it would give a helpful overview of the status quo of how networked the individual security systems of different cities are today. Then such data could possibly be correlated with data of various incidents (naturally caused and man-made) trying to determine whether the broad access to such data has helped the security

communities to either more quickly solve a criminal case or possibly avert economic damage and/or infrastructural losses via early detection of a possible threat or a faster reaction to the latter.

10. Special features/remarks: