OVERVIEW

Nearly a decade has passed since the President's National Security Telecommunications Advisory Committee (NSTAC) last reviewed the Nation's communications resiliency posture. In the *2011 NSTAC Report to the President on Communications Resiliency* (Communications Resiliency Report), the NSTAC examined the areas noted below:

- **Current Assessment:** An examination of the then-current communications interoperability and resiliency landscape.
- **Government Investment/Action Advice:** An analysis of potential Government actions to enhance the survivability and availability of communications for first responders and critical infrastructure operators in time of disaster.
- **Predicting Future Technology Trends and Anticipated Needs:** A study of future networks' resiliency in a disaster to identify predicted trends around: (1) future use; (2) service provisioning; (3) technology development; (4) network architecture; and (5) security.

COMMUNICATIONS RESILIENCY

"[T]he degree to which a network can withstand damages, thereby minimizing the likelihood of a service outage. Resiliency is the result of three key elements: (1) route diversity, (2) redundancy, and (3) protective and restorative measures (e.g., security)."[1]

TREND ANALYSIS

Many developments have transpired in the information and communications technology (ICT) ecosystem since 2011. The table below captures trend areas, the NSTAC's 2011 predictions, and their status today.

TREND	2011 NSTAC ASSESSMENT	CURRENT STATUS
Video and Multimedia	• Predicted rise in video, multimedia, and mobile devices with high data traffic	• Accelerating adoption of wireless, smartphones, and streaming
Applications	• Predicted the importance of social media and application stores/content aggregators	• Rise of containers, virtualization, and application programming interfaces transforming application development and creating new threats
Broadband and 4G	• Emphasized the growth of broadband and 4G	• Introduction of 5G and new 5G technologies, capabilities, and deployments • Rise of threat competition from China
Devices and Equipment	• Underestimated the growth of smartphones • Expected the cost of mobile devices to decline • Predicted the growth of machine-to-machine and Internet of Things (IoT) communications	• Hypergrowth in IoT devices • Saturation of smartphone/wireless devices • Virtualization of wireless infrastructure • Increase of open software and systems
Remote Workforce	• Emphasized workforce dispersion and presumed connectivity availability • Highlighted the importance of consumer broadband connectivity	• Uneven broadband coverage and connectivity continues in U.S. rural markets • Accelerating remote workforce putting pressure on availability of reliable remote access
Service Provider Consolidation	• Projected industry consolidation • Assumed a common network infrastructure (versus an open, non-proprietary approach) • Referenced greater geographic diversity of services	• Top-tier consolidation continues, with a proliferation in start-up/venture capital firms • Proliferation of new network technologies and architectures • Explosion in "over-the top" services, new business models, and virtual network providers

[1] SAFECOM/National Council of Statewide Interoperability Coordinators, *Public Safety Communications Network Resiliency Self-Assessment Guidebook*, Executive Summary iv, *November 2018,* https://www.cisa.gov/sites/default/files/publications/DHS%20ECD%20Public%20Safety%20Communications%20Network%20Resiliency%20Self-Assessment%20Guidebook_11.29.18%20-%20FINAL.pdf.

TREND	2011 NSTAC ASSESSMENT	CURRENT STATUS
Satellite and Global Positioning Systems Usage (GPS)	• Predicted satellite as alternative to terrestrial-based communications • Identified GPS as becoming imbedded in devices	• Development of High Throughput Satellites, Low Earth Orbit Satellite Mega Constellations, and enhanced GPS (eGPS) • Proliferation of non-U.S. GPS solutions • eGPS requirements, 5G networks, and big data improving location tracking
Identity Management (IdM)	• Highlighted stove-piped identity solutions • Defined IdM problem, but not a solution	• Increasing password/multifactor authentication vulnerability • Need for enhanced IdM solutions
Cloud Computing	• Identified cloud as "the new information infrastructure" • Flagged increased complexities for network management	• Accelerated adoption of multi-cloud and edge computing to support IoT and new applications • Cloud delivery model has gone mainstream

FUTURE STUDIES

In addition to reexamining the areas outlined in the above trend analysis, recent events—including the coronavirus (COVID-19) pandemic, California wildfires, and Midwestern floods---have highlighted novel challenges for communications resiliency. The dynamic nature of the ICT technology ecosystem further complicates this landscape. To examine the impact of these challenges, the NSTAC may revisit its 2011 Communications Resiliency Report and/or review the additional topic areas for consideration, noted below.

The NSTAC could prioritize a select set of topics of the below to establish a recommended examination schedule. These proposed topic areas are not exhaustive or mutually exclusive; the NSTAC may study certain topics together, examine them in tandem, and/or consider additional topics of interest based on the needs study.

Post COVID-19 pandemic review.

- What telecommunications issues have emerged during of the COVID-19 pandemic response? What emerging technology opportunities have been realized?
- What foreseeable impact will the pandemic have on the long-term management of the Nation's ICT supply chain?
- What strengths and weaknesses can be gleaned from the public and private sector's response? What opportunities for public-private sector collaboration have emerged as a result of the pandemic? What lessons can be learned for enhanced coordination in the future?

Cascading impacts of critical infrastructure interdependencies.

- Which critical infrastructure sectors pose the highest risk of failure during emergency situations? Which interdependencies are the highest priority to examine? What role do the National Critical Functions play?
- How has promoting continuity of communications (CONCOMM) capabilities evolved since 2011? Which recommendations in the 2011 NSTAC Communications Resiliency Report should be updated to address current critical infrastructure interdependencies?
- What communications and critical infrastructure coordination best practices from previous emergencies can be applied in the future?

Impact of 5G and emerging technologies.

- How do increasing numbers of communication points (e.g., towers) and decreased availability of landlines impact emergency communications?
- How do emergent capabilities (e.g., 5G networks, software-defined networking, LTE, next generation 911) impact emergency communications?
- How can emerging technologies address CONCOMM interdependencies and/or improve alert distribution?

Operational- and policy-level coordination needed to ensure accurate and timely alert distribution.

- What are the emergency communications needs of state, local, tribal, territorial, and private sector partners? How can the Federal Government better support these communications needs before, during, and after emergencies?
- What can the Government do to improve local and national emergency alert distribution (e.g., Executive Order, regulation, legislation)?
- What criteria should the Government consider when creating a prioritization schema for issuing targeted alerts, warnings, and notifications (AWN)?

Methods for issuing targeted AWNs to at-risk populations.

- What factors should be considered to ensure the correct audiences receive AWNs and act on the guidance received? What key information needs to be provided to emergency managers? Who is the authoritative source for this information?
- What gaps exist in industry standards for geotargeted AWN issuance (e.g., Alliance for Telecommunications Industry Solutions)?
- What cybersecurity risks should be considered with AWN?
- What influence does social media have on the ability to target communications during emergencies?