| SECURITY & STABILITY |
| --- |
| • Define sec. & stability first<br>• Facilitate defining what “security” means to the community (and what “community”)<br>• Define ICANN’s role in security and stability<br>• Inventory of what we and others do on security – who to call when you’ve fallen and can’t get up<br>• Definitions and community agreement on why “security and stability” is used at ICANN<br>• Change the language to healthy, sustainable, resilient<br>• Terminology is important<br>• Communicate role. Align<br>• Make this a central part of ICANN “brand” name association<br>• Change the framing of the issues<br>• Help users and gov’ts and corps VALUE their stable internet more<br>• Become the recognized technical expert other look to for solutions<br>• ICANN is to be a globally recognized expert on security, but not an IT consultancy<br>• More assertive of what we do and follow up on success<br>• ICANN as a convener of risk experts. Publicize ICANNS role<br>• Crisis management team function. Coordination<br>• Convening, scenario, discussions, planning<br>• Whatever we do, make sure community is consulted when necessary<br>• Training, education, awareness, thought leadership. Actions do support ICANN’ role.<br>• Engage with technology vendors to understand what ICANN can do to help<br>• Familiarity of engagement team with security issues<br>• What must ICANN do to ensure a secure & stable Internet with the complexity and reach anticipated in 2018<br>• Root servers. ICANN’s coordination function<br>• What do you need to improve quality?<br>• Mechanisms for staying ahead of developing technologies instead of reacting<br>• Demonstrate we recognize the importance of this function<br>• Raising operational capabilities of our security ops<br>• Adoption of security technology<br>• Strengthen developing country CCTLD operation. Best practices.<br>• 24hr capability<br>• One Internet. Avoid fragmentation.<br>• What types of things, activities would support a healthy, sustainable, resilient ecosystem?<br>• Greater use of advisory committees in this area (SSAC-RSSAC)<br>• Fractioning in terms to make ICANN’s role more acceptable (i.e. improve quality vs. control, security)<br>• Increase our alignment with gov’ts on security & stability<br>• Make education aspect of security priority or viable |

- Security missing in OEP
- Expand community & staff competencies/basic knowledge
- Training for broader community on security priorities
- Cert? DNS, root, etc.
- Ensure engagement in new technologies and new developments
- Ensure there is an environment of “no fear”
- Environment of harmony and diplomacy
- Be more proactive for example – ensure guidelines on human rights are followed
- Improve technical specifications by enhancing the backend and simplifying the front end for the end users of the DNS
- Enhance ability to take over failure or non-compliance on DNS held by registrars/registries
- Better compliance measurements and early warning systems to monitor registries/registrars.
- Have a model for takeover and determine level of failure.
- Enhance civil society role as a watchdog
- Increase lines of communication with organizations which deal with security issues (CERTs, etc.)
- More accurate WHOIS
- We need DANE to fix certificate problems. DANE will make ICANN’s SSR role vital
- What is answer to NSA US Snoop?
- There is still relative neglect of the African market in terms of region specific or country specific domains, let alone the security thereof, especially when the African market has such a huge market
- NSA Out
- There is need to get African Professionals to be engaged
- (Van Roste – CENTR; peter@centr.org) According to ICANN’s AOC (Affirmation to Commitment) signed on September 30th 2009 and the resulting 28 recommendations from the review team Security, Stability and Resiliency of the DNS (SSR RT) in their final report from June 2012, ICANN should develop a roadmap to enhance the operational stability, reliability, resiliency, security, and global interoperability of the DNS, which must be regularly updated by ICANN to reflect emerging threats to the DNS. The SSR RT was particularly paying attention to:
  a. security, stability and resiliency matters, both physical and network, relating to the secure and stable coordination of the Internet DNS;
  b. ensuring appropriate contingency planning; and
  c. maintaining clear processes.

  It is not clear if and how the recommendations from the SSR RT will be followed up by the Strategy Panel on Identifier Technology Innovation in the continuous work of ICANN. It is of CENTR’s opinion that the panel could benefit from building from prior work rather than start all over. Nevertheless ICANN also need to take a longer view at some of the challenges facing the DNS (beyond root key rollover). The most recent update from the SSR work was published in the appendix to the FY 14 SSR Framework.
  CENTR would like to point out the importance of respecting the existing diversity as an essential element of the overall security of the DNS.