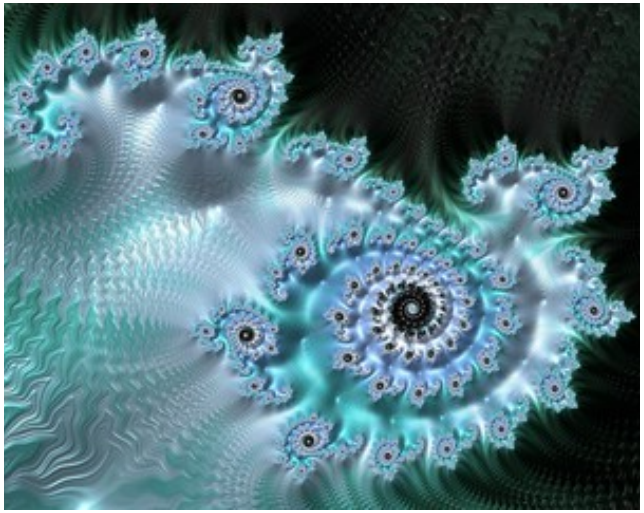
Complexity at High Speed

Summary: A VUCA world—volatile, uncertain, complex, and ambiguous—means that issues unfold both rapidly and in unexpected ways. Hyper-connectivity and automation compound the issues of speed and complexity. Social media causes the human side to operate at high speed as well: a company or an individual can go from unknown to globally controversial in a matter of hours.



Forecasts

- A VUCA world holds the danger that novel threats to the organization will be overlooked, because their indicators do not fit past patterns or expectations.
- The accelerating pace of change will force decision-makers to adapt to making effective decisions without the luxury of complete analysis. This will elevate the importance of timeliness in decision-making, based on the "best available evidence."
- The proliferation of data flows will increase the importance of identifying key metrics and indicators for potential threats, combined with real-time responsiveness.
- Accelerating change will cause small initial informational advantages to turn into substantial gains. Organizations will feel growing pressure to gather more information, process it faster, and act rapidly on that information to remain competitive with peers.

Key uncertainties for rapid change and complexity:

- Adoption rate and impact of artificial intelligence
- Degree to which social cohesion can be maintained in the face of polarizing forces
- Ability of governing institutions to effectively respond to rapid social and technological changes
- Impacts of growing global interconnectedness

Supporting trends

Fears of technology. Polling reveals that people are afraid of a variety of technological developments, such as cyberterrorism, identity theft, and government tracking of personal data.

Climate-change induced instability. Climate change is suspected of having rising impacts on national security and geopolitical stability.

Social media aids extremism. Social media has expanded the reach of fringe ideologies, enabling causes marginalized by the mainstream to exploit new media channels.

Technologies for faking audio and video. Researchers have developed technologies that can use a sample to generate synthetic speech based on a real individual, or animate an artificial face based on an actual individual in real time.

Precision violence. Precision targeting technologies are becoming increasingly available—even to civilians—in advanced drones.

Political polarization and class. Political polarization in the US is becoming more extreme between the highly educated and those with only a high school degree.

Social media as vectors for physical threats. Social media is being used by malicious actors to provoke violence.

Inequality of opportunity rising. Studies have documented widening gaps in opportunity as a function of socioeconomic status.

Data points

***Sudden, random threats*.** In 2018, Internet celebrity Kylie Jenner tweeted a negative comment about Snapchat to her 25 million Twitter followers. This tweet caused Snap Inc. stock to drop 8 percent in heavy trading, a decline in company valuation of nearly one billion dollars.

Cybercrime as a service. According to the security firm Carbon Black, "Comparing 2016 vs. 2017 YTD, the ransomware marketplace on the dark web has grown from $249,287.05 to $6,237,248.90, a growth rate of 2,502%." According to FBI data, ransomware extortion rose from $24 million in 2015 to nearly $1 billion in 2016. The "dark web" contains a growing number of competing ransomware portals, where users can find a variety of turnkey services for distributing, implementing, and collecting funds from ransomware attacks.

Topics for additional research

- Strengths and limitations of high-speed automated threat detection
- Systems for spotting novel threats

Strategic insights

For the security industry

- To respond effectively to a rapidly evolving threat environment, organizations may need to turn to more ad-hoc security teams. Such teams could gather to rapidly manage incidents as they emerge and evolve, and then disband when the issue is resolved.
- The new media environment is pushing organizational reputation into the security domain. The growing importance of issues management, framing, and perception management could blur the lines between public relations and psychological operations, and make such skillsets more valuable.
- An operating environment of growing complexity could require security professionals to acquire communications and digital marketing skills to more effectively defend against new threats. These skills could include social media literacy, data analytics, sentiment analysis, and social graphs.
- Uncertainty and change can boost the demand for security services. However, customer satisfaction is likely to require a suite of methods that address the underlying psychology as well as tangible threats.

For ASIS

- The "fake news" phenomenon is creating new demand for authoritative and objective experts. ASIS has the potential to have a larger role as a trusted source regarding security issues and wider security implications in areas such as news, training, and professional standards and guidelines.
- Accelerating change could have direct impacts on training programs. The AGOBA study could offer insights on impacted areas.

Timing

- **Stage**: Growing, in a period of expansion
- **Speed**: Moderate change, but with sudden bursts

Potential alternative futures

- **Air-gapping the net.** Widespread dissemination of sophisticated hacking tools pushes many organizations to move critical information to systems with no direct connections to the Internet.
- **The new normal.** People adapt to a changing environment, and adjust their expectations of normality accordingly.
- **Hunger for stability.** Increasing instability leads to a growing demand for security at any price.
- **Power of the flock.** Accelerating change unlocks new patterns of self-organization and creates new foundations for stability.