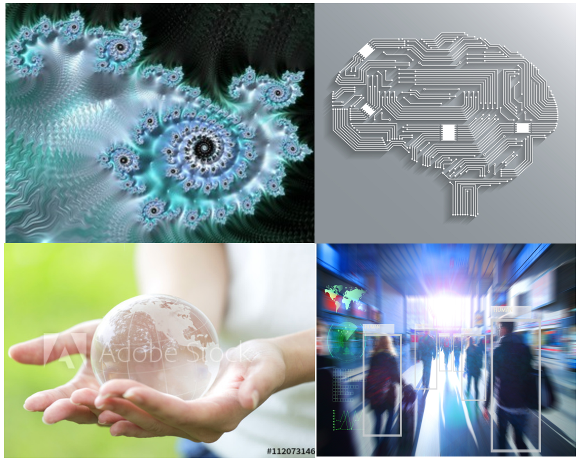
ASIS Scouting the Future

Summary: Terror attacks, data breaches, ransomware—there is constant need for security, but the form it takes is evolving in the face of new technological capabilities and social and geopolitical changes. The seven change drivers identified in this research are by no means a comprehensive outlook for the future of security, but represent areas where change is occurring most rapidly and could have the largest impact. These change drivers derive from a foresight best-practices approach that spans technology, geopolitics, social issues, economics, and the environment.



Intended use

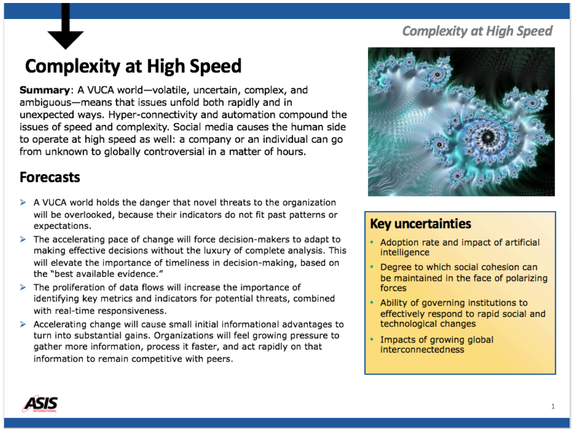
- For the ASIS Board of Directors: The research can inform an ongoing process of strategic planning to set priorities that enable leadership of the security profession.
  - For the Strategic Planning Committee: The research can surface strategic opportunities for ASIS.
  - For the ASIS Content Strategy Team: The research can form the basis of content to disseminate through the association's multiple channels to educate and inform ASIS members.
- For the ASIS Foundation Board of Trustees: The research can guide investments in research initiatives to update and deepen the profession's body of knowledge.
  - For the Foundation Research Committee: The research can support a research agenda that prioritizes and defines proposed research initiatives.

The process

- Interviewed ASIS members for their understanding of the terrain of interest
- Developed domain map defining the areas to be investigated
- Researched 80 trends and signals of change, and provided over 100 additional background trends
- Developed 15 potential change driver ideas as a result of analysis of the trends
- Honed change driver ideas based on advisory board and ASIS member feedback
- Produced the seven change drivers, with periodic reviews by advisory board

Elements of a Change Driver

- **Page 1** provides an overview of the change.
  - **Summary paragraph**: This is a concise description of the driver of change. It can be used in reports, summaries, or other information flows to describe the brief.
  - **Forecasts**: Based on the trends and data points collected, these are primary forecasts of changes in this topic area. They represent what are known as “probable futures”—the changes that are more likely to happen given current trends and data.
  - **Key uncertainties:** In any forecast area, there are uncertainties that can alter the future. These are the “known unknowns,” and they need to be considered when making downstream forecasts.



Complexity at High Speed

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

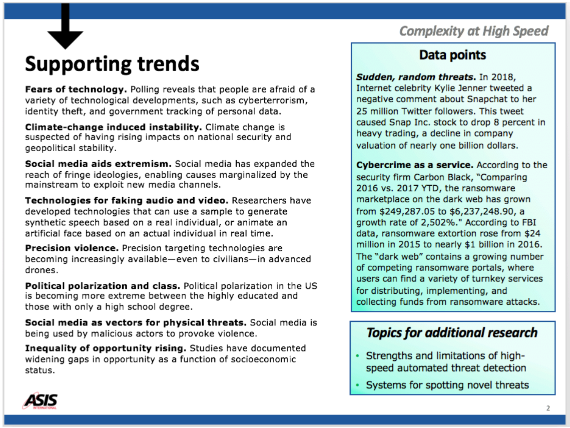
- A VUCA world holds the danger that novel threats to the organization will be overlooked, because their indicators do not fit past patterns or expectations.
- The accelerating pace of change will force decision-makers to adapt to making effective decisions without the luxury of complete analysis. This 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

- 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

1

- **Page 2** provides more detailed support for the change.
  - **Supporting trends**: These are key trends and weak signals that drive this change and provide background understanding of the rationale for the forecasts and other sections.
  - **Data points:** These are a few interesting data points that illustrate and support the change.
  - **Topics for additional research**: These indicate candidates for more in-depth research.



Complexity at High Speed

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.

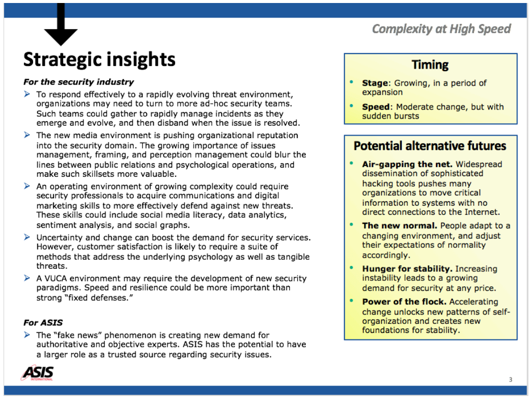
Topics for additional research

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

2

Elements of a Change Driver

- **Page 3** provides ideas to seed strategic planning discussions.
  - **Strategic insights**: These implications are divided into two categories: for the security industry and for ASIS as an association.
  - **Timing:** Timing identifies the overall maturity and speed of the driver of change, in order to understand priority and urgency: stage, which assesses where the change driver is in its lifecycle; and speed, which addresses how fast or slow the driver is moving.
  - **Potential alternative futures:** These are some possible (not probable) futures that should be considered from a risk-management perspective.



Complexity at High Speed

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.
- A VUCA environment may require the development of new security paradigms. Speed and resilience could be more important than strong "fixed defenses."

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.

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.

3

Change Drivers

The change drivers describe seven areas of change that are important for ASIS to understand as the organization develops strategic plans and provides leadership in the security industry.

Complexity at High Speed: 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.

Shifting Values and Valuables: Technological, generational, and economic changes are reshaping ideas about what is valuable. In particular, information—especially in digital forms—is becoming more central to corporate functions and peoples' lives. Organizations will have to navigate diverging views of risk, and security will have to continually adjust to what is seen as worth protecting.

Global Rules in Flux: International rules are evolving as power shifts and new actors arise. How global politics, business, trade, technology, and even science are governed will inevitably change, as the needs and perspectives of the newly powerful are accommodated. Some systems will be adjusted, and others may be overturned.

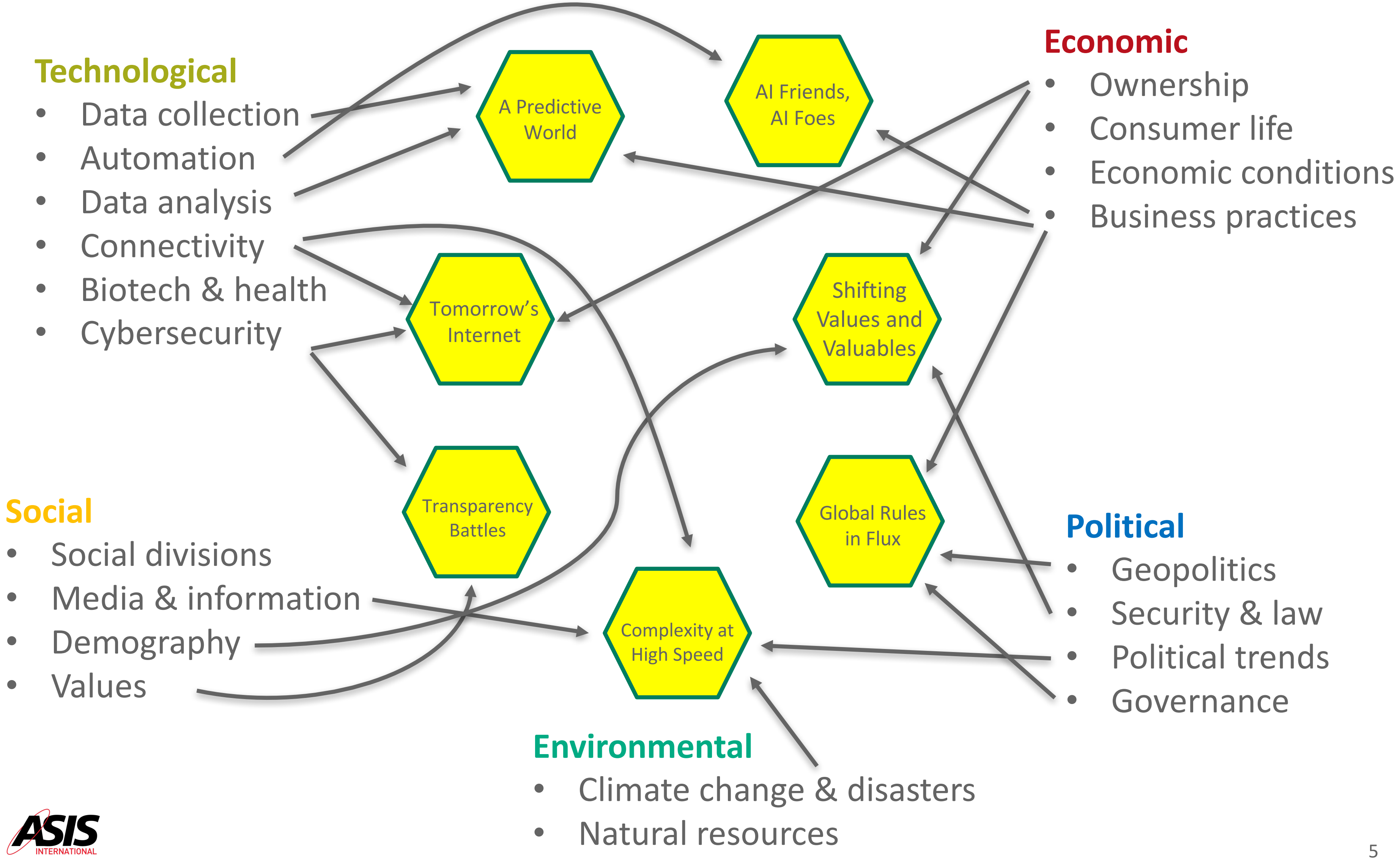
Tomorrow's Internet: The Internet is poised to change in multiple, potentially radical ways. New regulatory frameworks could significantly alter the user experience as well as the business models behind it. Moves to give end users more ownership and control over their personal data would reshape online marketing and security, and the growth of the Internet of Things will give network connectivity to objects in the physical environment.

AI Friends, AI Foes: AI systems will become central to ever more activities, with human-machine cooperation increasingly pervasive in business and industry. Automation will enhance security by enabling new types of threat detection and response. However, these tools in the hands of malefactors will expose and create new vulnerabilities in systems previously thought secure. Forecasts Automation could increase the general public's expectation.

A Predictive World: Predictive analytics will provide low-cost, easy-to-use tools to businesses, organizations, and individuals. This will empower users with a greater ability to detect and forecast developments to make better-informed decisions, but these systems could also provide false or skewed information that may distort choices.

Transparency Battles: Transparency is increasing, for companies, governments, and individuals, and is in conflict with needs for privacy and secrecy. In a more transparent world, organizations will face a growing expectation of openness and accountability in their decision-making, relationships, and practices.

Spanning the Forces of Change



Technological
- Data collection
- Automation
- Data analysis
- Connectivity
- Biotech & health
- Cybersecurity

Economic
- Ownership
- Consumer life
- Economic conditions
- Business practices

A Predictive World

AI Friends, AI Foes

Tomorrow's Internet

Shifting Values and Valuables

Transparency Battles

Global Rules in Flux

Complexity at High Speed

Social
- Social divisions
- Media & information
- Demography
- Values

Political
- Geopolitics
- Security & law
- Political trends
- Governance

Environmental
- Climate change & disasters
- Natural resources

Conclusion

The security industry and ASIS will face many challenges in the years ahead, but find abundant new opportunities as well. Understanding the implications of the changes outlined in these briefs will allow them to navigate the evolving environment and develop the strategies needed to lead in the new, emerging future.

Some challenges and opportunities for the **security industry** include:

- ✓ New models of risk assessment and cost evaluations that focus on changing ideas of what is valuable and needs to be protected
- ✓ Recognizing that information technology and as a consequence cybersecurity is pervasive across an organization, thus changing the whole administrative framework for security services within an organization
- ✓ The widespread use of artificial intelligence, and as a consequence the evolving role of security in both leveraging and protecting against machine interactions
- ✓ Evolving legal and social issues around balancing security needs with individual rights and expectations in surveillance, privacy, encryption, etc.
- ✓ Managing the new media environment with special focus on issues and perception management

A few of the challenges and opportunities for **ASIS** include:

- ✓ Educating and guiding members through the technology adoption and learning curve for AI, predictive analytics, and digitally-empowered social environments
- ✓ Expanding its global influence in defining security best practices, guidelines, and standards
- ✓ Increasing public and corporate awareness of the changing nature of security threats, tensions, and solutions