Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS

armasuisse
Sciences et technologies

DEFTECH Update

Avril 2017

Cher Lecteur,

Ce document résume les signaux faibles en rapport aux technologies émergentes fournis par les services *Scan* et *Explorer* de la société Strategic Business Insights' (SBI) auxquels le Programme de veille technologique d'armasuisse Sciences + Technologies est abonné.

Pour chaque tendance, nous avons anticipé une possible opportunité ou menace pour les forces armées et indiqué quelles capacités devrait être la plus directement impactées. Chaque tendance est également reliée à son signal faible correspondant décrit en anglais. Ces signaux originaux constituent la seconde partie de ce document.

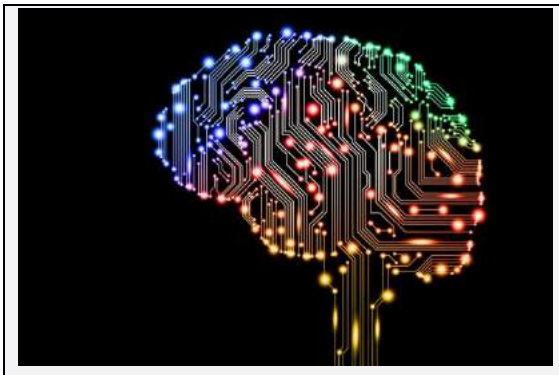
Le but recherché par cette publication est de sensibiliser chaque lecteur aux innovations technologiques en cours tout en adoptant un format plaisant et lisible rapidement. Bien que vous ayez sûrement déjà entendu parler de bon nombre de ces technologies, laissez-vous surprendre par la convergence de nouveaux domaines !

J'espère que vous apprécierez le voyage!

Meilleures salutations,

Dr. Quentin Ladetto
Directeur de recherche – Veille Technologique

P.S. Pour tout commentaire, suggestion ou discussion: quentin.ladetto@armasuisse.ch



IA en Chine

Les développements récents de l'intelligence artificielle (IA) ainsi que les investissements massifs en Chine accompagnent des politiques industrielles et militaires en pleines mutation laissant présager des perspectives alarmistes sur l'utilisation de l'AI. Par exemple, des développement sont en cours en Chine sur les essaims de drones intelligents, des sous-marins autonomes ainsi que des missiles de croisière enrichis d'IA.

***Implications Défense et Sécurité**: La Chine fait toujours face à des obstacles quant à la réalisation de la parité avec l'Occident en termes de ressources IA, mais elle s'améliore rapidement et devient compétitive. L'abondance des activités militaires liées à l'IA en Chine pose des défis pour les combattants occidentaux qui cherchent à profiter des avantages uniques de l'évolution de l'IA.*

***Délais d'implication:** maintenant/5 ans/**10 ans**/15 ans*

***Capacités:** L'utilisation de l'intelligence artificielle peut impacter toutes les capacités.*

Interfaces Cerveau-Machine

Les interfaces cerveau-machine progressent; en particulier avec les interfaces permettant le contrôle des mouvements et des sensations tactiles. Ces interfaces sont très utiles pour les prothèses et peuvent également servir au contrôle de la robotique, y compris les exosquelettes et les jeux informatiques.

***Implications Défense et Sécurité:** Les interfaces cerveau-machine pourrait permettre aux soldats de communiquer de manière silencieuse, de contrôler des armes par la pensée, ou de reprendre le combat après une blessure, la perte d'un membre ainsi que l'utilisation de prothèses. Les interfaces cerveau-machine pourraient également faire progresser la formation au combat des soldats.*

***Délais d'implication:** maintenant/5 ans/**10 ans**/15 ans*

***Capacités:** Sanitaire (5.2), Conduite*

L'emprise du Hacking s'élargit

La vulnérabilité des dispositifs de l'Internet des objets (IoT) et les grandes bases de données constituent des menaces majeures pour la vie privée ainsi que pour la sécurité physique des utilisateurs. Par exemple, en novembre 2016, des pirates ont utilisé Internet des objets pour monter une attaque de déni de service distribué (DDoS) contre le système de chauffage d'un bloc d'appartements en Finlande alors que la température extérieure était de -10°C . Ces dispositifs, faciles d'utilisation, sont également faciles à pirater et à coupler à des botnets.

Implications Défense et Sécurité: *IoT utilisés par le personnel de la défense sont attrayants pour les attaquants, et offrent des possibilités aux pirates pour l'obtention de renseignements, pour la prise de contrôle des fonctions et des opérations essentielles, ou la communication délibérée de désinformation. Les zones particulièrement vulnérables incluent la sécurité des véhicules, les soins de santé - tels que le matériel de surveillance médicale contrôlé à distance - et les chaînes d'approvisionnement.*

Délais d'implication: ***maintenant****/5 ans/10 ans/15 ans*

Capacités: *Protection des armes et des appareils (6.2), sécurité des ouvrages (6.3), Effet dans le cyber-espace (3.5)*

Gestion de l'espace

Les orbites autour de la Terre sont de plus en plus congestionnées par des pays et entreprises privées lançant des satellites ainsi que par la prolifération de petites charges utiles spatiales peu coûteuses. Cette congestion augmente la probabilité de collisions. L'inquiétude au sujet de cette situation est de plus en plus grande parmi les différents opérateurs, en particulier dans l'industrie des télécommunications. .

Implications Défense et Sécurité: *la congestion spatiale représente une menace pour les organisations de défense et de sécurité qui reposent sur des satellites pour la surveillance et les communications. À l'avenir, les exploitants de systèmes spatiaux seront vraisemblablement responsables de la désaffectation complète de leurs produits spatiaux à la fin de leur durée de vie opérationnelle. De nouvelles possibilités existent par l'intermédiaire de senseurs et grâce à la puissance informatique embarquée d'obtenir un statut instantané du satellite et ainsi permettre la gestion en temps réel de la situation spatiale « globale ».*

Délais d'implication: ***maintenant/5 ans/10 ans****/15 ans*

Capacités: *En fonction de type de satellite ou de constellation affecté, cela peut avoir un impact sur toutes les capacités.*

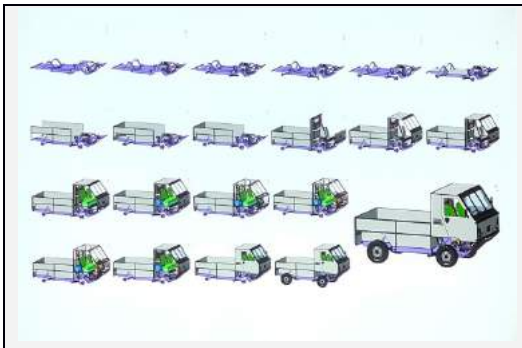
Le marché des matériaux thermoélectriques se développe

La start-up Matrix Industries (Menlo Park, Californie) a créé ce qu'elle prétend être le premier smartwatch au monde qui ne nécessite pas de rechargement. La PowerWatch s'appuie sur un générateur thermoélectrique utilissnt la différence entre la température du corps de l'utilisateur et la température du boîtier métallique de la montre pour créer un courant électrique.

Implications Défense et Sécurité: *Les appareils électroniques portables ainsi que les équipements de surveillance de la santé fonctionnant en continu et sans recharge pourraient être bénéfiques pour le personnel de sécurité et militaire sur le terrain. Les générateurs thermoélectriques peuvent également alimenter en continu capteurs et caméras utilisés pour la surveillance et la collecte de renseignements dans des endroits distants ou difficiles d'accès.*

Délais d'implication: ***maintenant/5 ans*** */10 ans/15 ans*

Capacités: *Sanitaire (5.2), Recherche d'information (2.2)*



L'économie des produits "lego" (flat-packs)

Des entreprises explorent les avantages de la logistique et des coûts pour la construction de véhicules à base de composant « plats et assemblables ». Le philanthrope Torquil Norman et le concepteur de voitures de course Gordon Murray ont travaillé ensemble pour développer le « Ox » (bœuf) ; un camion tout-terrain facile à assembler qui peut transporter jusqu'à 13 personnes et 1 900 kilogrammes de cargaison, et pouvant être démonté en 60 parties en 12 heures.

Implications Défense et Sécurité:. *Ce type de véhicules, plus faciles et moins coûteux à transporter par rapport aux véhicules entièrement assemblés, pourrait permettre d'économiser de l'argent et du temps aux militaires dans le transport de véhicules et par conséquent d'autres équipements également.*

Délais d'implication: *maintenant/**5 ans**/10 ans/15 ans*

Capacités: *Mobilité (4.1-4.2), Logistique (5.1)*

Opportunités dans l'espace

Les efforts gouvernementaux et commerciaux visant à mesurer (et contrôler ?) un large éventail d'activités à partir de l'espace deviennent de plus en plus courants, car la miniaturisation et la diminution des coûts de la technologie spatiale permettent l'utilisation de satellites de plus en plus petits pour obtenir un regard de plus en plus précis sur notre Terre.

Implications Défense et Sécurité: *La prolifération de petits satellites représente une occasion de décentraliser (et/ou dupliquer) des réseaux de communications et de surveillance par satellite, les rendant moins coûteux et moins vulnérables aux attaques.*

Délais d'implication: ***maintenant**/**5 ans**/10 ans/15 ans*

Capacités: *Information et communication (1.5), Recherche d'information (2.2), Diffusion des renseignements (2.4)*

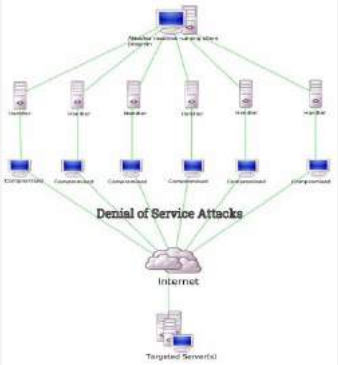
Curieux robots commerciaux

Les chercheurs continuent de développer des fonctionnalités robotiques apparemment impossibles qui pourraient étendre les domaines d'application des robots. Par exemple, les chercheurs de la Walt Disney Company (Burbank, Californie) ont développé un robot à une jambe capable de se déplacer par sauts grâce à ses senseurs et une algorithmique complexe.

Implications Défense et Sécurité: *Les progrès dans les senseurs et la puissance de calcul disponible à très petites dimensions facilitent le développement de robots militaires agiles en mesure d'effectuer des actions complexes dans divers environnements.*

Délais d'implication: *maintenant/**5 ans**/**10 ans**/15 ans*

Capacités: *Efficacité à l'engagement, Recherche d'information (2.2), Logistique (5.1), Protection individuelle (6.1)*



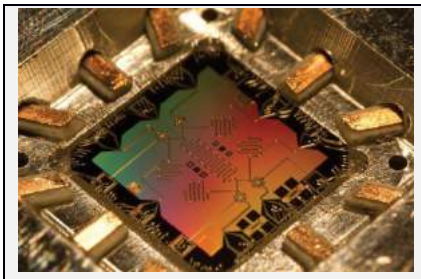
Prolifération des attaques DDoS

La prolifération d'outils de piratage peu coûteux et facilement disponibles a rendu possible le lancement d'attaques distribuées de déni de service (DDoS) pour quasiment tout le monde. Un certain nombre de grandes entreprises ont signalé avoir connu une série d'attaques DDoS de plus en plus sophistiquées.

Implications Défense et Sécurité: *les attaques DDoS ont la possibilité de désactiver des plates -formes et services Web ainsi que des dispositifs distribués(IoT) perturbant ainsi le bon déroulement des opérations. Les attaques DDoS peuvent également être des écrans de fumée pour les attaques plus malveillants.*

Délais d'implication: ***maintenant**/5 ans/10 ans/15 ans*

Capacités: *Conduite, Service de renseignement, Effet dans le cyber-espace (3.5), Autres appuis (5.5), Sécurité des informations et des données (6.4)*



Disruption par le cryptage quantique

Bien que les ordinateurs quantiques sont encore à quelques années de leur commercialisation, les chercheurs font des progrès avec les matériaux, les conceptions et les méthodes nécessaires pour les créer. Différentes organisations gouvernementales et entreprises travaillent cependant déjà à l'informatique quantique à pleine échelle et au cryptage quantique.

Implications Défense et Sécurité: *Il existe des opportunités pour tirer parti de l'informatique quantique afin de sécuriser les communications et protéger leur réseaux contre le piratage. À l'inverse, le calcul quantique avec ses nouvelles capacités de chiffrement pourrait constituer une menace pour les organisations de défense et de sécurité qui s'appuient sur des stratégies de chiffrement « classique », ce qui crée un besoin d'anticipation dans le développer d'algorithmes post-quantiques.*

Délais d'implication: *maintenant/5 ans/**10 ans**/**15 ans***

Capacités: *Information et communication (1.5), sécurité des informations et des données (6.4)*

Caméras omniprésentes

Les caméras deviennent omniprésentes et utilisables dans une grande variété d'applications. La société Snap (Los Angeles, Californie) prévoit de commercialiser des lunettes de soleil qui utilisent une caméra intégrée pour prendre des photos et enregistrer des vidéos.

Implications Défense et Sécurité: *L'intégration des caméras dans les articles portables classiques fournit un moyen discret de surveillance et de collecte de renseignements et permet également la documentation des interventions.*

Délais d'implication: ***maintenant****/5 ans/10 ans/15 ans*

Capacités: *Information et communication(1.5), Recherche d'information (2.2), Instruction (5.4)*

STRATEGIC BUSINESS INSIGHTS

EXPLORER

Viewpoints

March 2017

Artificial Intelligence

By Michael Gold (mgold@sbi-i.com)

AI in China

Why is this topic significant? Recent developments are driving increased expectations for China's competitiveness in business and military applications of AI.

Description

Recent artificial-intelligence- (AI-) related technology developments and investments in China accompany shifts in that nation's industrial and military policies, motivating bullish views about the outlook for AI there. China-based start-ups enjoying recent large venture-capital investments include aspiring cloud-robotics service CloudMinds ($100 million during February 2017) and computer-vision specialist SenseTime ($120 million during December 2016). Other interesting business cases include those of robotics developer NineBot, speech and natural-language specialist Iflytek, and analytics-software supplier 4Paradigm. KPMG consultants predicted that Chinese AI companies will see a major uptick in venture investments during 2017.

February 2017 news articles indicated that China's government is funding or incentivizing the establishment of a national AI lab in the form of a consortium that search giant Baidu leads and that includes a number of research institutes and universities. During October 2016, a public-private partnership began construction on a 10-square-kilometer, $275 million facility for testing unmanned commercial and military vehicles. *Unmanned* (无人) also describes additional recently reported development efforts toward intelligent drone swarms, autonomous watercraft, and AI-enhanced cruise missiles.

China's AI researchers have been busy for some years. Baidu assembled its own AI lab in 2013; in 2016, messaging giant Tencent did likewise, as did ride-hailing company Didi Chuxing. An October 2016 report from the White House asserted that among all nations, China's researchers published the greatest number of cited journal articles about deep learning during 2014–15, and Japanese software and services company Astamuse recently presented data indicating 186% growth in the annual number of applications for AI-related patents in China in the five year period ending in 2014, outpacing such growth in any other region (the actual annual number of AI patent applications in China remained only about half that of the United States at the end of the period).

Implications

China still faces obstacles to achieving parity with the West in terms of AI resources, but the nation is rapidly improving its competitiveness. At a minimum, domestic AI developments enjoy favorable prospects because language forms natural barriers to entry in meeting needs for natural-language processing and because censorship policies are effectively protectionist, benefiting Baidu and Tencent while disadvantaging Google, Facebook, and other AI leaders. And although China's military has much catching up to do, an abundance of military-related AI activities in China poses challenges for Western warfighters who seek to enjoy unique advantages from AI developments.

Impacts/Disruptions

Factors that inhibit AI innovation in China include lack of academic freedom and limits to entrepreneurs' abilities to field technologies that might disrupt social cohesion there. Nevertheless, China's pent-up supply of talent might transcend me-too technologies, fielding world-class innovations in certain aspects of AI—plausibly, in machine translation, which still needs much more progress, and in intelligent military systems to deny access to specific places such as within disputed offshore boundaries. Analysts also cannot rule out a "Chinese century" scenario in which that nation eventually does indeed overtake others in AI and other domains by surpassing Western nations in terms of public funding for advanced R&D and by redoubling its domestic base of AI talent and its considerable recruitment of top talent from the rest of the world.

Scale of Impact	Low	Medium	**High**	
Time of Impact	Now	5 Years	**10 Years**	**15 Years**

Opportunities in the following industry areas:
Machine translation, driverless vehicles, military systems, drones, computer vision, robotics, speech recognition, natural-language processing, cloud services

Relevant to the following Explorer Technology Areas:
• Artificial Intelligence • Big Data • Collaboration Tools • Connected Cars • Pervasive Computing
• Robotics • User Interfaces

STRATEGIC BUSINESS INSIGHTS

EXPLORER

Viewpoints

March 2017

Artificial Intelligence

By Sean R. Barulich and Michael Gold (mgold@sbi-i.com)
Barulich is a research analyst with Strategic Business Insights.

AI versus Cancer

Why is this topic significant? Increasingly, research and early commercialization efforts focus on cancer—part of the overall growth in AI-health-care research and business development. AI promises to amplify health-care capabilities, from new drug research to specific patient analysis and treatment planning.

Description

For decades, physicians have used various artificial-intelligence (AI) technologies to research new drugs, sequence genes, and diagnose diseases, including cancer. Current R&D projects and early commercialization efforts plan to do even more with intelligence-driven health-care solutions.

Microsoft is engaged in a range of AI applications that focus on improving cancer treatment, spanning diagnosis, combination-drug therapy, radiology, and management of chronic cancers. Google DeepMind is working to improve the process of safely identifying and removing tumors while saving tissue. US Defense Advanced Research Projects Agency contractors are investigating use of machine learning and semantic technologies in a search for the causes of cancer in the massive quantity of preexisting medical research. Other organizations that have recently reported progress in advanced research about use of AI for cancer care include Cornell University, the University of Chicago, and start-up Insilico Medicine.

Some signs point to increased commercialization of AI for helping cancer patients. IBM and Quest Diagnostics introduced a service that recommends combination drug therapies and treatment plans for various cancers. Start-up Flatiron Health's OncoAnalytics tool reportedly applies machine learning and natural-language processing to aggregated research and patient data from cancer centers, with an aim of making clinical trials more effective. Another start-up—Zebra Medical Vision—recently claimed it outperformed human radiologists' abilities to detect early-stage breast cancer.

Implications

AI can serve to dig through large medical data sets and discover significant health information more quickly than humans can. Use of AI technology

promises to improve accuracy of radiological diagnosis and radiotherapy, effectiveness of novel drug combinations, and identification of cutting-edge cures now undergoing trials. Hopes are also high for AI to contribute to *personalized medicine*—formulation of individualized treatment and disease-management plans that take into consideration the particular ailment, the patient's health history, genetics, and other factors.

Impacts/Disruptions

AI's role in oncology is likely to grow along with other roles in medicine, but the nature of the role—and whether its contribution is altogether positive—is highly uncertain. Ideally, AI-health-care applications may amplify health-care capabilities—speeding diagnosis, identifying effective remedies, improving quality of life for patients with debilitating forms of the disease, and even reducing costs of care. But events sometimes expose stakeholders to be overoptimistic, as in the case of a failed $62 million project to use IBM's Watson at the University of Texas MD Anderson Cancer Center.

Computer vision might have heterogeneous effects on the practice of oncology, with individual surgeons, specialists, clinics, and insurers having individual levels of trust in machines and human diagnosticians. Impacts on demand for radiologists are also uncertain. Behind the scenes, radiological diagnosticians seem to take advantage of AI as a tool, but AI's ultimate effects could be to reduce growth in the profession or even erode it.

Outcomes for highly personalized cancer treatments are also uncertain. Today, such treatments (Apple's Steve Jobs was a famous recipient) don't necessarily rely on new AI technologies but involve doctors' sequencing cancer genes and searching for drug combinations and other therapies that can remedy specific sequences. Imaginably, AI could play roles in popularizing such therapies. Alternatively, automation might speed diagnosis and treatment but still mainly benefit wealthy patients who can afford such meticulous care.

Scale of Impact	Low	Medium	**High**	
Time of Impact	**Now**	**5 Years**	10 Years	15 Years

Opportunities in the following industry areas:
Biotechnology, drug research, health care, software development

Relevant to the following Explorer Technology Areas:
• Artificial Intelligence • Big Data • User Interfaces

STRATEGIC BUSINESS INSIGHTS

EXPLORER

Viewpoints

March 2017

User Interfaces

By Rob Edmonds (redmonds@sbi-i.com)

Brain–Machine Interfaces: An Update

Why is this topic significant? Elon Musk says that humans need upgrading with brain–machine interfaces. Superintelligent humans that merge with AI remain firmly fictional, but electronics and software can repair and enhance specific brain functions.

Description

Tesla CEO Elon Musk claims that human intelligence must merge with machine intelligence to compete with artificial intelligence. Musk is optimistic about future brain–machine interfaces and claims to be working on "neural laces." Various research groups are apparently researching ultrafine mesh electronics for brain interfaces—presumably the technology Musk envisions.

Although neural laces do not yet exist, brain-machine interfaces are already useful.

- In early 2017, researchers lead by Niels Birbaumer of the Wyss Center for Bio and Neuroengineering in Geneva, Switzerland, used a brain–machine interface to record yes/no answers from four people with no voluntary muscle movement. The skull-cap interface used near-infrared spectroscopy to monitor blood flow and electrical waves.

- "Progress toward Brain Implants" in the February 2016 Viewpoints outlines progress toward the use of invasive procedures for creating thought-controlled user interfaces for prosthetics and robotics.

- University of Southern California researchers are due to start testing electrode implants to aid the formation of long-term memories (the team receives funding from the US Defense Advanced Research Projects Agency's effort to develop memory prosthetics).

- Although commercial electroencephalography (EEG) headsets have reliability problems, successful applications exist. For example, in 2016, the University of Florida used EEG headsets to hold the world's first brain-controlled drone race.

Implications

Brain interfaces are progressing, but current technologies involve compromise. Users must choose among invasive procedures, bulky and

impractical skullcaps, and unreliable headgear. These compromises tend to limit current brain interfaces to medical applications and to toys, games, and novelties. New technologies, including mesh electronics, are important research areas.

Some brain functions are proving easier to interface with than others. In particular, scientists are having success in interfacing with motion control and touch sensations. These interfaces are very useful for prosthetics and can also serve robotics control (perhaps including exoskeletons) and computer games. Some researchers have made progress toward motion-control brain interfaces for larger objects, including cars (though reliability and safety issues likely make such developments long term).

Scientists are also progressing with interfaces to other specific brain functions. Control of speech synthesizers is possible, and verbal communication with deeply paralyzed patients is a breakthrough. Researchers are at the early stages of developing memory prosthetics, and the technology could plausibly help patients with memory-related conditions.

Impacts/Disruptions

Although some brain–machine interfaces are remarkable, the idea that human and machine intelligence could "merge" into some form of superintelligence is still firmly in the realms of science fiction. Plausible brain–machine interfaces could improve memory, remotely control robots, and transmit verbal information. But the road map to brain interfaces that can receive information telepathically, accelerate brain processing, or increase intelligence is far from clear. Indeed some brain interfaces may overwhelm people rather than enhance them (for example, concentrating on remotely controlling a robot while performing another task). And, for most people, "telepathy" may turn out to be a far less efficient way of receiving information than reading or listening (for example, one of the few brain-to-brain experiments transmitted "information" with an on/off brain stimulation that participants experienced as a flash of light).

Scale of Impact	Low	Medium	**High**	
Time of Impact	Now	5 Years	**10 Years**	15 Years

Opportunities in the following industry areas:
Smartphones, wearables, electronics, software services

Relevant to the following Explorer Technology Areas:
• Artificial Intelligence • Human Augmentation • Pervasive Computing • User Interfaces

STRATEGIC BUSINESS INSIGHTS

EXPLORER

Viewpoints

March 2017

User Interfaces

By Rob Edmonds (redmonds@sbi-i.com)

The Handover Problem for Autonomous Vehicles

Why is this topic significant? Balancing driver attention and autonomous features is a significant user-interface challenge for semiautonomous vehicles. In particular, multiple tests show that handing control from a car to a human driver is difficult. Although some companies think they can solve this handover problem, others aim to move straight to driverless technology.

Description

The US National Highway Traffic Safety Administration reported it found no defects in Tesla's Model S safety systems after investigating a fatal crash that occurred in 2016. However, US Transportation Secretary Anthony Foxx said that manufacturers need to be clear about the limits of semiautonomous systems, and lawyers warn that manufacturers still need to be concerned about liabilities for collisions when cars control themselves. Despite the uncertainties, Tesla is pressing ahead with a phased rollout of autonomous driving technology. The company plans to issue software updates to add autonomous driving features to Tesla cars as it develops them. For the foreseeable future, these features will require drivers to be on standby to regain control of the vehicle.

Other developers of autonomous vehicles are bypassing semiautonomous driving technologies and aiming to move straight to vehicles that require no driver input. The results of Google's handover tests in 2013 led the company to focus on fully autonomous driverless vehicles. Ford is also planning to move straight to fully autonomous vehicles. Ford technical leader for autonomous vehicles, Jim McBride, says "We're not going to ask the driver to instantaneously intervene—that's not a fair proposition."

Other manufacturers believe that they can solve the handover problem. Volvo's two-pronged strategy involves driverless and semiautonomous cars. Audi plans to bring hands-free, eyes-free semiautonomous driving to its 2018 model-year A8. Audi plans to install systems that monitor driver attention and issue alerts that drivers will see, hear, and feel.

Implications

Although driver-assist technologies have been around for years, carmakers are facing new user-interface challenges as autonomous technology arrives—and the handover problem is particularly difficult. Unlike machines, people behave unexpectedly, lose concentration, start checking messages, and even fall asleep. Technologies exist to monitor and predict driver alertness, but many of these technologies are almost as challenging to create as driverless technology itself.

Impacts/Disruptions

Incremental software updates that gradually increase autonomy are risky. Such updates make cars unpredictable, perhaps confusing drivers about their vehicles' autonomous behavior and the requirement for driver input. Tesla's history of deploying "beta" software is also a concern. "Beta products shouldn't have such life-and-death consequences," says Steve Wozniak, cofounder of Apple, who owns a Tesla Model S.

Other applications of artificial intelligence and robotics also face handover problems. Humans may need to respond to problems among large teams of manufacturing robots or take over from a customer-service bot dealing with a serious complaint or unravel an automated-trading strategy gone awry. Autonomous military systems likely also have handover problems with significant consequences. Handover is one of many user-interface challenges that engineers need to solve as the artificial-intelligence and robotics markets develop.

Scale of Impact	Low	Medium	**High**

Time of Impact	Now	**5 Years**	10 Years	15 Years

Opportunities in the following industry areas:
Automotive, artificial intelligence, robotics, electronics, software services

Relevant to the following Explorer Technology Areas:
• Artificial Intelligence • Connected Cars • Pervasive Computing • Robotics • User Interfaces

STRATEGIC BUSINESS INSIGHTS

scan™

March 2017

P1036

Hacking's Reach Expands

By Ivona Petrache (Send us feedback.)

Security breaches are becoming increasingly harmful, and manufacturers of vulnerable devices are beginning to face legal challenges.

Abstracts in this Pattern:

SC-2017-02-01-054 on account information
SC-2017-02-01-028 on heating system
SC-2017-02-01-014 on DDoS attacks
SC-2017-02-01-059 on IoT platform
SC-2017-02-01-009 on legal action

Vulnerable Internet of Things (IoT) devices and large databases are becoming major threats to the privacy and even the physical safety of users. In October 2016, hackers attacked FriendFinder Networks (Campbell, California), which operates Adult FriendFinder and several other adult online services and websites. The hackers exploited system vulnerabilities and stole and published information from some 400 million accounts. And in November 2016, hackers used IoT devices to mount a distributed-denial-of-service (DDoS) attack against the heating system of an apartment block in Finland. The hackers created a cycle of attacks by disabling the heating system every time the system rebooted. Because the attacks occurred during 20°F weather, the lack of heating posed a physical threat to building residents.

By selling IoT devices that are easy for consumers to use, manufacturers are also selling devices that are easy to hack and incorporate into botnets. In October 2016, a large botnet consisting of webcams and other IoT devices fueled two DDoS attacks on internet-services provider Dyn (Oracle Corporation; Santa Clara, California). The attacks disrupted Dyn's service for several hours, and the websites of companies such as Twitter (San Francisco, California) and Amazon.com (Seattle, Washington), which depend on Dyn's services, were temporarily inaccessible as well. In the future, such hacks may necessitate legislation that addresses the security of IoT devices.

Companies are working on increasing the connectivity of IoT devices. For example, Yamaha Corporation (Hamamatsu, Japan) has launched Advanced Robotics Automation—a platform that connects IoT devices. The platform may decrease the cost of automated production lines and increase compatibility among IoT devices. But the vulnerabilities of IoT devices with poor security have caught the attention of lawyers. For example, two class-action suits claim that the connectivity of vehicles from various car manufacturers could enable hacking and endanger public safety. Other industries—including the toy and medical-device industries—may also be vulnerable to IoT-related class-action suits. Whether such legal challenges will slow the proliferation of insecure, hackable IoT devices or encourage increasingly imaginative end-user license agreements is unclear.

Signals of Change related to the topic:

SoC886 — Putting the IoT in Perspective
SoC875 — Hacking to Manipulate
SoC797 — Internet of (Growing) Threats

Patterns related to the topic:

P1021 — Proliferating DDoS Attacks
P0571 — Internet of Threats
P0359 — …Security Tug-of-War

STRATEGIC BUSINESS INSIGHTS

scan™

March 2017

SoC932

Managing Space Junk

By Cassandra Harris (Send us feedback.)

Earth's orbit is becoming increasingly congested because more and more countries and companies are launching satellites into orbit, and small, inexpensive space payloads are proliferating (P0948 — Space Invaders provides related information). This congestion increases the likelihood that collisions will occur, and such collisions could have catastrophic consequences and leave an even greater amount of debris in orbit. Concern about this situation is growing among operators of government and commercial space systems and companies in a variety of industries—especially the telecommunications industry. The effective management and removal of orbital debris requires international coordination, and who will pay for efforts to address orbital congestion remains unclear.

Despite the many commercial activities that occur in space, space remains a difficult environment to work in. In March 2016, Japanese astronomy satellite Hitomi lost contact with ground control and disintegrated just one month after its launch. An investigation by the Japanese government concluded that human error and inadequate project programming by the Japan Aerospace Exploration Agency (JAXA; Tokyo, Japan) were responsible for the loss of the satellite. The investigation also revealed that JAXA's internal organization was not equipped to handle the large projects the agency was working on. Earth's orbit is home to the world's fleet of communication and navigation satellites. Damage to or the loss of these satellites can have serious implications for essential terrestrial operations, and incidences of human error by space-system operators and potentially deliberate attacks on satellites pose a significant threat to national security. In 2013, the Chinese military launched what it claimed is a space-exploration rocket, but the US Department of Defense (Arlington County, Virginia) claims that China was actually testing antisatellite technology.

Plans exist for the launch of at least 3,600 new satellites in the next decade.

Organizations are looking toward using small satellites for commercial and research purposes. For example, start-up Planet Labs (San Francisco, California) operates a large constellation of *CubeSats*—small space-research satellites comprising one or multiple cube-shape units that weigh less than 3 pounds each. These CubeSats orbit Earth to collect images of terrestrial activities for use in a variety of applications, including market research, natural-resource monitoring, and disaster relief. Small satellites are creating additional commercial opportunities. For example, Vector Space Systems (Tucson, Arizona) is developing a rocket specifically for frequently launching small satellites into space. In 2014, the Unites States conducted only 23 orbital launches, but Vector aims to conduct hundreds of orbital launches per year.

Millions of pieces of debris—including discarded equipment from old satellites, tools, and pieces of rockets—are moving within Earth's orbit at speeds as great as 28,000 kilometers per hour. These pieces of debris can collide with operational spacecraft and satellites, causing catastrophic damage that creates showers of smaller pieces of debris. For example, the 2009 low-Earth-orbit collision between an operational US-built commercial satellite and a deactivated Russian-built military satellite created an estimated 2,000 pieces of debris. After the collision, the US military became the leading provider of data about *space situational awareness (SSA)*, which the website of the Space Foundation (Colorado Springs, Colorado) describes as the ability to identify and track the locations of human-made and natural objects that are orbiting Earth in efforts to prevent collisions.

At present, the Joint Space Operations Center (Vandenberg Air Force Base, California) uses the US Space Surveillance Network (SSN)—a system that comprises ground radar and optical systems and satellite-based sensors and falls within the purview of the US Department of Defense (Arlington Country, Virginia)—to track space debris and provide space-system operators around the world with collision-warning notifications and statistical analysis. However, the SSN can track only objects with a diameter of 10 centimeters (cm) or larger. In low Earth orbit, according to NASA (Washington, DC), "the estimated population of particles between .4 inches and 4 inches (1 to 10 cm) in diameter is approximately 500,000. The number of particles smaller than .4 inches (1 cm) probably exceeds tens of millions" (www.nasa.gov/news/debris_faq.html). NASA highlights that pieces of debris as small as flecks of paint can tear through satellites and space stations as they travel through space at extremely high velocities. The US Air force contracted Lockheed Martin (Bethesda, Maryland) to construct the Space Fence—a new space-object-tracking radar capable of tracking pieces of orbital debris that are much smaller than those that existing systems can track. After it commences operations in 2018, the Space Fence will be capable of tracking an estimated 200,000 objects, including marble-size pieces of debris in low Earth orbit. Although the capabilities of the Space Fence will be an improvement over those of the SSN, tracking space debris can go only so far in preventing collisions. Measurements of the trajectories of pieces of space debris are often uncertain, and space-systems operators are currently under no legal obligation to perform collision-avoidance maneuvers with their space-based assets.

Researchers are also developing new technologies capable of removing debris from Earth's orbit. For example, JAXA is developing a space-debris-disposal system that comprises a spacecraft and a 700-meter-long electrodynamic tether. The craft will deploy the tether and guide it toward large pieces of space debris. Once the tether captures the piece of debris, the craft will drag the object into Earth's atmosphere, which will incinerate both the object and the spacecraft. Because the system focuses on the disposal of pieces of space debris ranging from about 400 to 4,000 pounds, it will not remove the numerous tiny pieces of debris that fall outside the SSN's tracking capabilities.

Plans exist for the launch of at least 3,600 new satellites in the next decade, and many of these new satellites are CubeSats and other small satellites. This increase in the number of such satellites orbiting Earth will significantly complicate the already challenging tasks of ensuring the safety of orbital operations and preventing collisions and other disasters. Large financial benefits exist in protecting space-based assets, and opportunities exist to leverage advances in sensor technologies and computing power to enhance SSA-system capabilities. However, many aerospace-industry players believe that a central authority is necessary to enforce space-system operators' liability for the full decommissioning of space assets at the end of their operational lifetimes. Donald Greiman, vice president and general manager of commercial SSA at the Schafer Corporation (Arlington, Virginia), believes SSA duties should transfer from the US Air Force to the US Federal Aviation Administration (FAA; Washington, DC), which is an agency of the US Department of Transportation (Washington, DC). According to Greiman, the FAA is "the only agency that can put safety as number one and has the government association to protect the information" ("Many questions, few answers when it comes to space traffic management, experts say," *SpaceNews*, 17 January 2017; online).

SoC932

Signals of Change related to the topic:
SoC922 — Opportunities in Space
SoC615 — Space-Commerce Bubble
SoC189 — Space-Based Commerce

Patterns related to the topic:
P0948 — Space Invaders
P0646 — Private Space
P0166 — Where There Is Space…

STRATEGIC BUSINESS INSIGHTS

scan™

March 2017

P1043

The Market for Thermoelectric Materials Expands

By Marianne Monteforte (Send us feedback.)

New commercial ventures indicate that substantial potential exists to expand the market for thermoelectric materials.

Abstracts in this Pattern:
SC-2017-02-01-008 on NASA
SC-2017-02-01-077 on Matrix Industries
SC-2017-02-01-073 on FutureSiSens

The market for thermoelectric materials could be very large in a variety of industry sectors, including aerospace, wearable electronics and sensors, and health care. In the aerospace domain, researchers from the NASA (Washington, DC) Jet Propulsion Laboratory are developing skutterudite thermoelectric materials for use in the agency's next-generation nuclear-battery system. Skutterudite materials are particularly beneficial for capturing waste heat from industrial applications and converting that heat into electrical energy. The NASA researchers believe the materials can also find use in nuclear batteries, which use the waste heat from the radioactive decay of plutonium-238 as the power source. According to the researchers' analyses, the skutterudite-based nuclear-battery system will generate 25% more power than do the nuclear-battery systems currently in use and require smaller amounts of expensive plutonium-238.

Commercial applications of thermoelectric materials are beginning to emerge in the realm of wearable electronics. Start-up Matrix Industries (Menlo Park, California) has created what it claims is the world's first smartwatch that does not require charging. The PowerWatch smartwatch relies on a thermoelectric generator for power, and the generator uses the differential between the temperature of a wearer's body and the temperature of the watch's metal housing to create an electric current. Because the PowerWatch can very precisely measure changes in a user's skin temperature, it can use temperature changes to calculate how many calories a wearer burned during a workout—in effect, the thermoelectric generator can act as a sensor.

Meanwhile, researchers from the Autonomous University of Barcelona (Cerdanyola del Vallès, Spain) and two other institutions in Spain created spin-off FutureSiSens (Cerdanyola del Vallès, Spain) to commercialize their new thermoelectric microsensor. The researchers based the device, which can sense minute changes in gas flow, on silicon nanotechnology, and the device is so sensitive that it can "pick up a variation of temperature measured in millikelvins in someone's breathing rhythm." The sensor has many potential applications in the health-care industry, but it may also find use in the defense and mining industries.

Signals of Change related to the topic:
SoC910 — Origami-Inspired Design…
SoC778 — …Materials' Production and Selection
SoC739 — Healing Materials

Patterns related to the topic:
P1013 — …Lithium-Ion Batteries
P1003 — Altering Adhesion
P0348 — Nanoscale Energy Harvesting

STRATEGIC BUSINESS INSIGHTS

scan™

February 2017

P1028

Economics of Flat-Pack Products

By Cassandra Harris (Send us feedback.)

Companies are developing affordable flat-pack housing and vehicles.

Abstracts in this Pattern:
SC-2017-01-04-103 on Modulhus
SC-2017-01-04-017 on Big World Home
SC-2017-01-04-002 on Ox

Companies are exploring the logistics and cost advantages of flat-pack buildings. For example, Barton Willmore (London, England) and Ecomotive (Bristol, England) have developed Modulhus—a flat-pack home that consists of 15-by-9-foot prebuilt modules that fit together to create a stand-alone home, terrace, or low-rise apartment block. The standard two-bedroom, 710-square-foot Modulhus home costs as little as £49,644 ($60,000). Such ready-to-assemble homes could help people climb onto the property ladder despite housing shortages and rising house prices; however, buyers of such homes must also purchase land, which can be limited and expensive—particularly in urban areas. Similarly, Big World Homes (http://bigworldhomes.com) develops small, flat-pack, off-grid homes for the Australian residential market and is trying to make purchasing property easier. Big World Homes partners with community groups, developers, and property owners "to find land spaces from unused plots to backyards where one Big World Home or a pop-up community can be erected." The houses sell for $60,000 to $80,000 Australian dollars ($45,000 to $60,000 in US dollars), and easy access to online support enables even people without building experience to erect a Big World Home using only a drill and a hammer.

Other designers are looking at extending the advantages of flat-pack logistics into the realm of vehicles. Philanthropist Torquil Norman and race-car designer Gordon Murray worked together to develop the Ox, which is an easy-to-transport all-terrain flat-pack truck for use in the developing world. The Ox can carry as many as 13 people and 4,100 pounds (1,900 kilograms) of cargo but can break down into 60 parts within 12 hours. Shipping the Ox in its flat-pack form is much less expensive than shipping a standard fully assembled vehicle.

Signals of Change related to the topic:
SoC701 — Flexible Offices
SoC691 — Origami Engineering
SoC685 — Next-Generation Manufacturing

Patterns related to the topic:
P0875 — Printing Architecture
P0836 — Transforming Cargo Transportation
P0528 — Frontier Product Delivery

STRATEGIC BUSINESS INSIGHTS

EXPLORER

Viewpoints

February 2017

Artificial Intelligence

By Michael Gold (mgold@sbi-i.com)

Intelligent Image Processing

Why is this topic significant? Behind the scenes, image-processing algorithms are critical enablers for digital video and photography. Progress in algorithms promises to support next-generation needs for compression and image enhancement.

Description

In dozens of TV shows and movies, a detective or hacker examines a blurry image on a computer screen; someone utters "enhance" and through the magic of software, a clue is revealed in the resulting sharpened image. During November 2016, a team of researchers from Google and the Technion-Israel Institute of Technology published research findings about the restoration of lost details in images. Researchers trained the algorithm with high- and low-resolution versions of some 10,000 existing images. The resulting trained system processes new images by applying nuggets of wisdom about the relationships among similar images at different resolutions.

Google researchers exhibited some examples of enhanced images having doubled, tripled, or quadrupled resolution in each dimension; the algorithm presents a noticeable improvement relative to several hitherto state-of-the-art methods. Moreover, Google reports that the algorithm excelled in speed of operation. The researchers acknowledged significant contributions to prior art by others, including a team from the Chinese University of Hong Kong and Microsoft Research, and another team from ETH Zurich and Katholieke Universiteit Leuven.

According to Google, by January 2017 the Google+ social network had begun to employ essentially the same algorithm for a converse task: reducing the data requirements to store and deliver pictures. Google reported that it was processing more than a billion images weekly for certain Android users, reducing the data required to transmit the images by about one-third relative to previous practices.

Implications

Without compression, users would require huge increases in storage and bandwidth resources to enjoy personal digital photo albums and streaming video. Assuming Google's claims about image compression hold in a general way, similar algorithms could compress video content more effectively than algorithms now used in practice. Or

conversely, improved algorithms could increase resolution of standard-definition video content to serve high-definition displays, and increase resolution of high-definition content to serve ultra-high-definition (UHD) displays. (Respectively, algorithms could upscale 480p video to 1080p, or could upscale 720p video to 4K.)

Recent trends may be pointing to increased demand for improved video-image quality. An increasing share of new TV sets include displays that present some combination of UHD, brighter whites and blacker blacks (increased dynamic range), and increased range of colors (wide color gamut). Improved compression could be important for delivering higher-quality images while reining in requirements for increased storage and bandwidth.

The image-enhancement capabilities of Google's algorithm could also help adapt existing content, making it look good on ultra-resolution displays, and avoiding the pixelated and block-shaped artifacts that appear in similar situations. And no doubt, detectives, persons with blurry photos of loved ones, and other parties would see high value in even relatively limited abilities to restore lost details to images.

Impacts/Disruptions

Progress in image compression signals that further progress may be possible toward related goals. Stakeholders might use learning algorithms to further reduce the resources required to store and process audio, text, databases, and other data structures.

Google's algorithm does not rely on deep learning or artificial neural networks, and in fact it appears to have surpassed a predecessor deep-learning algorithm in terms of both computational efficiency and resulting image quality. Such an outcome illustrates that deep learning is not necessarily the "master algorithm" that solves every difficult problem.

Scale of Impact	Low	**Medium**	High	
Time of Impact	**Now**	**5 Years**	10 Years	15 Years

Opportunities in the following industry areas:
Digital photography, video production and distribution, surveillance, data archives

Relevant to the following Explorer Technology Areas:
• Artificial Intelligence • Big Data • Collaboration Tools • Connected Cars • Connected Homes
• Electronic Displays • Mobile Communications • Pervasive Computing • Robotics • User Interfaces

STRATEGIC BUSINESS INSIGHTS

EXPLORER

Viewpoints

February 2017

Artificial Intelligence

By Michael Gold, with contributions by Sean R. Barulich (mgold@sbi-i.com)
Barulich is a research analyst with Strategic Business Insights.

Testing the Safety of Driverless Vehicles

Why is this topic significant? Questions remain unresolved about how to prove that driverless cars will become safe enough for common use. Similar questions could apply to safe use of other intelligent systems that will appear in the future.

Description

During September 2016, Nvidia Corp. published a video demonstration of a car operating autonomously at night on a poorly marked dirt road and in other challenging environments. The following month, Tesla Motors announced that all the cars it manufactured at that point "have the hardware needed for full self-driving capability at a safety level substantially greater than that of a human driver," and Nvidia indicated it is now the main AI hardware supplier for Tesla (which until recently relied on Mobileye). In a late 2015 *Fortune* article, Tesla CEO Elon Musk expressed confidence in Tesla's effort: "It's a much easier problem than people think it is. But it's not like … a one-guy-and-three-months problem. You know, it's more like, thousands of people for two years."

In contrast, separate 2016 reports from Rand Corporation and Carnegie Mellon University researchers expressed concerns about proving the safety of driverless vehicles: Statistically significant safety demonstrations could require billions of miles of testing—an impractical undertaking. Alternative ways to assure the safety of driverless cars could require extensive use of redundant systems, onboard monitoring of system behavior, stress tests (including deliberate injections of faulty data), and phased deployments involving gradually increasing semiautonomous capabilities.

Implications

Many people express hope for driverless cars to operate when no passenger is competent to drive and for unoccupied vehicles to deliver themselves to waiting passengers. But many questions remain about self-driving capabilities in poor weather and heavy traffic; when vehicles merge, change lanes, and pass at freeway speeds; and where road markings are poor or hazards are present.

Principles of statistics and mathematical rules governing large numbers indicate that makers of fully autonomous cars "cannot drive their way to

safety" (in the words of the Rand Corporation researchers). But insurers and others still need a reason to believe that driverless cars come with acceptable risks.

Different models of vehicles and software updates could trigger need for repeated rounds of safety testing. Use of machine-learning systems in safety-critical applications is unprecedented, further complicating needs for safety verification. Cost and weight considerations impose practical constraints on use of redundant systems. Accompanying design rules and safety trade-offs could call for further design-verification efforts.

Impacts/Disruptions

In a better world, fully driverless vehicles might emerge only after engineers perfected mobile service robots that safely interact with people, factory robots that do not need to reside behind safety fences, intelligent heavy equipment such as bulldozers, and other relatively slow-moving mechatronic solutions to outstanding problems in robot safety. But strong market forces are prioritizing the first truly widespread use of robots in the form of 1,000 kg vehicles that commonly travel at over 100 km/h in public settings.

Are researchers' concerns about safety excessive? Perhaps today's computer technology is adequate to realize visions of unoccupied cars picking up blind people and children and delivering them safely to their destinations via any public road and under any weather conditions that human drivers now handle. Nevertheless, several design phases might precede the ideal, as stakeholders in general become progressively more confident in the safety of various modes of advanced assisted driving, driverless vehicles that operate in restricted areas and conditions, and other precursors of full autonomy.

Scale of Impact	Low	Medium	**High**	
Time of Impact	Now	5 Years	**10 Years**	**15 Years**

Opportunities in the following industry areas:
Transportation, mechatronics, cyberphysical systems, factory automation

Relevant to the following Explorer Technology Areas:
• Artificial Intelligence • Big Data • Collaboration Tools • Connected Cars • Mobile Communications
• Pervasive Computing • Robotics • User Interfaces

STRATEGIC BUSINESS INSIGHTS

scan™

February 2017

SoC922

Opportunities in Space

By Guy Garrud (Send us feedback.)

Government and commercial efforts to surveil a wide range of activities from space are becoming increasingly common as miniaturization and decreasing costs of satellite technology enable the use of smaller and smaller satellites to achieve an increasingly accurate look at the world from above. And telecommunications and broadcasting satellites are becoming increasingly important to keeping information flowing. Although the Space Age started half a century ago, opportunities in space continue to proliferate.

A range of industries already make strong use of satellite-imagery analysis. Planet Labs (San Francisco, California) has launched a small constellation of *CubeSats*—small space-research satellites comprising one or multiple cube-shape units that weigh less than 3 pounds each—and provides commercial satellite-imaging services. The company recently signed an agreement with geoanalytics firm Orbital Insight (Palo Alto, California), which uses satellite images to monitor sites that can provide useful economic information. For example, Orbital Insight can offer estimates about oil inventories by measuring the height of floating oil-tank lids in satellite images of oil-storage sites and measure the success of retail outlets by analyzing changes in the number of cars present in satellite images of parking lots. The company's software can also analyze satellite images of construction sites and cornfields to mine potentially useful data about various types of market information. Until it began working with Planet Labs, Orbital Insight received new satellite images for use in its analyses only monthly or bimonthly; however, under the new agreement, Planet Labs will provide Orbital Insight with new satellite imagery every week. In addition, if Planet Labs' plans to launch several dozen more CubeSats are successful, the company will provide Orbital Labs with new satellite images daily. An enabling component of Planet Labs' plans is that technological advances have enabled the manufacture of commercial satellites that are much lighter, smaller, and cheaper than are previous-generation commercial satellites. Furthermore, CubeSats weigh only a few pounds and are therefore easier and cheaper to launch into orbit than are conventional satellites, which can weigh several tons.

The satellite industry is growing synergistically with the space-launch industry.

The most common application areas for commercial satellites are telecommunications and media broadcasting. Most satellites still use radio signals to communicate; however, advances in free-space optical communication—which makes use of the movement of light through free space to transmit various types of data wirelessly—could open up new commercial opportunities. For example, China launched the world's first quantum-communications satellite in August 2016. The satellite operates using the principal of quantum entanglement, which states that a particle's transition from one quantum state to another correlates with the transitions of another particle, and the change in correlated particles at any distance occurs faster than light can travel between the two entangled particles. To encrypt signals, the satellite relies on quantum key distribution, which "works by transmitting particles of light called photons prepared in a particular quantum state. By measuring these states, the receiver on the other end can agree a stream of 0s and 1s that form a secure code or key, which can be used to encrypt data sent via conventional means—over the internet or through an ordinary communications satellite" ("Why quantum satellites will make it harder

for states to snoop," *New Scientist,* 24 August 2016; online). Because measuring a quantum system disrupts and changes that system, quantum communications are extremely difficult for a party to hack into without detection and therefore provide a very high level of security. Quantum-communication satellites could enable a new and lucrative market for telecommunications satellites, which in recent years have faced strong competition from terrestrial telecoms infrastructure that uses copper and fiber-optic cables to transmit data.

The satellite industry is growing synergistically with the space-launch industry: Growing demand for orbital launches supports increases in the number of companies that build and use rockets. SpaceX (Hawthorne, California) has been quite disruptive in recent years by offering orbital launches at a cost lower than those of traditional launch providers. The company has also gained considerable attention for its efforts to land and reuse the first stage of its Falcon 9 rockets. SpaceX has achieved substantial cost reductions without reusing its rockets, but the safe landing and relaunch of space hardware could cause launch costs to fall even further. Slashing the cost of launches has put SpaceX in a potentially very powerful competitive position; however, the company, which Elon Musk founded, is not the only organization pursuing cheap launches and reusable space hardware. Blue Origin (Kent, Washington)—a rocket company founded by Amazon.com (Seattle, Washington) CEO Jeff Bezos—is also testing the launching and landing of rockets. So far, all of Blue Origin's tests have been suborbital launches, which are much less technologically challenging than are low-Earth-orbit launches. However, Blue Origin recently announced that it hopes to put payloads into orbit with its next generation of launch vehicles. Vector Space Systems (Tucson, Arizona), which was founded by two members of the founding team of SpaceX, is targeting a subset of the commercial-launch market by developing rockets that can carry small payloads of a few kilograms into orbit. By offering dedicated launches for small satellites, the company can offer timely launches that place satellites into orbits that meet clients' specific needs. This approach offers advantages over the current approach of placing small satellites as additional payload on large launches, which limits small-satellite operators' choices for launch times and eventual orbits.

Several factors are working together to transform the satellite industry. Advances in sensors and energy-efficient electronics are enabling manufacturers to reduce the size and cost of satellites. And the expense of orbital launches is decreasing because of both technological development and increasing competition in the private-launch sector. In addition, companies are looking at innovative ways to make use of satellites and, consequently, increasing the demand for orbital launches.

A boom in the satellite industry also presents new challenges. For example, a growing number of satellites in orbit increases the likelihood that accidental collisions will occur. This situation is particularly important for orbits such as low Earth orbits and geostationary orbits, which are the most useful to satellite operators and therefore highly vulnerable to becoming overcrowded. Tracking and coordinating satellites and other objects in orbit is an increasingly difficult challenge.

SoC922

Signals of Change related to the topic:
SoC615 — Space-Commerce Bubble
SoC594 — Ultimate Cartography
SoC189 — Space-Based Commerce

Patterns related to the topic:
P0948 — Space Invaders
P0646 — Private Space
P0166 — Where There Is Space…

STRATEGIC BUSINESS INSIGHTS

scan™

February 2017

P1030

Peculiar Robotics of Commercial Interest

By David Strachan-Olson (Send us feedback.)

Distinctive robots and robotic features are beginning to see development and commercialization.

Abstracts in this Pattern:

SC-2017-01-04-031 on protecting
SC-2017-01-04-033 on insulating
SC-2017-01-04-052 on hopping
SC-2017-01-04-058 on sweating

The widespread availability of robotics components, rapid-prototyping equipment, and effective programming tools is enabling a broad range of individuals and companies to prototype unconventional robots for use in novel applications. In previous years, companies may have considered such novel robots too speculative to warrant the significant cost of their development; however, stakeholders can now rapidly design, develop, and commercialize such robots with relatively little investment.

A team at Hardshell Labs (La Honda, California) has built multiple remote-control rovers for use in protecting desert-tortoise populations that are under threat from predatory ravens. Volunteers use a web application to maneuver the rovers remotely and scare away the ravens. The team used off-the-shelf components in the design and construction of the rovers to minimize the cost of development. The team is also developing a mobile app that will enable users to control fixed laser arrays to scare away ravens. Start-up Q-Bot (London, England) has created a small foldable robot that travels in the hard-to-reach spaces under houses to apply insulating foam to the underside of the floor, eliminating the need for installers to rip up floorboards. The robot "can be inserted into hard-to-reach places through an air vent…. Once deployed, the robot is operated via remote control, allowing it to build a 3D picture of the space. Insulating foam is fed to the bot through a tube, so that the operator can spray the underside of the floor to seal up any gaps."

Researchers are continuing to develop seemingly impossible robotic features that could further expand robots' application areas. For example, researchers at The Walt Disney Company (Burbank, California) have developed a one-leg hopping robot that relies on sensors and a complex algorithm to balance itself. This robot demonstrates the capabilities of modern sensing and computing hardware, which could eventually enable the development of agile robots that can jump or run rather than shuffle or roll. Meanwhile, a team from the JSK Lab at the University of Tokyo (Tokyo, Japan) has developed an advanced humanoid robot that can sweat to control its body temperature. The researchers used an additive-manufacturing process to create a porous metal exoskeleton that circulates water for evaporation to improve cooling. Without this cooling, the robot's motors would quickly overheat and fail.

Signals of Change related to the topic:

SoC906 — Enabling Robotic Skills
SoC712 — …Commercial Footprint
SoC607 — Robotics: Up Close and Personal

Patterns related to the topic:

P0731 — Robot Motions
P0597 — Robotic Helpers across Industries
P0478 — Robotics' Spin-Offs

STRATEGIC BUSINESS INSIGHTS

scan™

February 2017

P1021

Proliferating DDoS Attacks

By Ivona Petrache (Send us feedback.)

Distributed-denial-of-service (DDoS) attacks are becoming easier to launch and therefore increasingly worrisome.

Abstracts in this Pattern:

SC-2017-01-04-053 on Mirai
SC-2017-01-04-018 on censorship
SC-2017-01-04-025 on Brian Krebs
SC-2017-01-04-001 on Bruce Schneier

In recent years, the proliferation of inexpensive and readily available hacking tools has made launching DDoS attacks possible for essentially anyone. For example, a hacker recently released the source code for Mirai—malware that enables users to hijack unsecured Internet of Things (IoT) devices such as internet-connected webcams and create a vast network of machines that can see use to mount DDoS attacks on websites. Because Mirai encrypts the internet traffic between the controlling servers and the hijacked devices, tracking down the source of such attacks is very difficult for security researchers.

The combination of cheap and easy-to-access hacking tools and the growing number of vulnerable IoT devices also democratizes censorship by enabling anyone to mount DDoS attacks against magazines and individual journalists. In September 2016, a large DDoS attack rendered http://krebsonsecurity.com —the website of cybercrime journalist Brian Krebs—inoperable for more than a day. The DDoS attack harnessed hijacked PCs and IoT devices with poor security to send more than 600 gigabits of junk data per second to the web-hosting servers that Krebs's site runs on, completely overwhelming them. Because Krebs regularly writes about the people behind DDoS attacks and the people who operate spam-email services and the like, his website is a frequent target of such cyberattacks.

In the past couple years, a number of major companies have reported experiencing a series of progressively more sophisticated DDoS attacks. These attacks—which appear to be coming from a particular set of locations—have the hallmarks of a coordinated probing of US cyberdefenses. For example, the attacks use a variety of methods, they take place over several weeks, and they become progressively more powerful, as if the attacker is trying to identify the target's vulnerabilities. According to computer-security expert Bruce Schneier, these attacks are "designed to determine exactly how well these companies can defend themselves, and what would be required to take them down." The attacks might indicate a ramp-up to the launch of massive DDoS attacks that would have a tremendous impact on organizations.

Signals of Change related to the topic:

SoC902 — Unusual Hacking…
SoC875 — Hacking to Manipulate
SoC797 — Internet of (Growing) Threats

Patterns related to the topic:

P0789 — …Possibilities for Cyberexploits
P0359 — The Internet of Things' Security…
P0256 — Hacking Incentives

STRATEGIC BUSINESS INSIGHTS

scan™

February 2017

SoC926

Quantum Computing's Security Disruption

By Rob Edmonds (Send us feedback.)

Quantum-computing researchers hope that the principles of quantum physics will enable radical innovations in computer architectures. Conventional computing relies on collections of binary nodes—that is, nodes that are in only one of two states at a time. Using the principles of quantum superposition and quantum entanglement, quantum computing can use collections of many-state particles (qubits) to create computing speeds that are much faster than those that rely on binary nodes.

The principle of *quantum superposition* holds that a subatomic particle can, despite people's intuitions, be in two seemingly contradictory states at once—for example, spinning in multiple directions simultaneously. In other words, in addition to being 0 *or* 1, a quantum particle can be 0 *and* 1. *Quantum entanglement* is another principle that violates common sense but, like superposition, has never failed to reveal itself in physics experiments that test the principle. A particle's transition from one quantum state to another correlates with the transitions of another particle, and the change in correlated particles at any distance occurs faster than light can travel between the two entangled particles. Entanglement enables collections of many-state particles—for example, two entangled particles encode superpositions of four states (00, 01, 10, and 11) rather than two (for a single particle).

Start-ups and large companies are working toward full-scale quantum computing.

Although full-scale quantum computers are still years away, researchers are making progress with the materials, designs, and methods necessary to create them. Toward the end of 2015, researchers at the University of New South Wales (Sydney, Australia) created—for the first time ever—a logic gate (a basic computation unit) using two entangled qubits composed of silicon. Previous qubit calculations used ultracold superconductors rather than the more stable and user-friendly silicon. The researchers patented a chip design that includes millions of qubits and has the potential to combine many qubit logic gates to perform complex computations.

Start-ups and large companies—including Google (Alphabet; Mountain View, California), IBM (Armonk, New York), and Microsoft (Seattle, Washington)—are also working toward full-scale quantum computing. For example, Google has hired noted quantum-computing researcher John Martinis to head up the company's efforts to build a workable general-purpose quantum computer. In late 2015, Dr. Martinis estimated that his team could build a workable general-purpose quantum computer with 100 qubits in as little as two years. Quantum-computing specialist D-Wave Systems (Burnaby, Canada) already offers a 1,024-qubit quantum computer, but the D-Wave design is capable of solving only a particular class of computing problems. In fact, quantum-computing experts are still debating whether D-Wave's machine actually provides any real advantage over conventional computers.

Quantum computing could find use in fields such as medical research, intelligence gathering, artificial intelligence, finance, and logistics. But quantum computing is particularly well suited for use in the field of information-technology security, and the arrival of full-scale quantum computers could be disruptive to this field. Scientists expect that full-scale quantum computing will excel at factoring large numbers, which is the basis of much current encryption. Indeed, some experts estimate that within 20 years, quantum computing could break all public-key encryption now in use, which concerns some stakeholders. For example, the nonprofit

Cloud Security Alliance (Seattle, Washington) warns that this development could have a disastrous effect on the global economy.

Although no one knows precisely when quantum computers will emerge, Michele Mosca of the Institute for Quantum Computing at the University of Waterloo (Ontario, Canada) believes that a one-in-seven chance exists that a fully functional quantum computer will arrive by 2026. The first full-scale quantum computer could even arrive in secret, enabling the entity that possesses it to decrypt almost any encrypted content and therefore gain significant advantages over its adversaries. The US National Security Agency (Fort Meade, Maryland) has been attempting to create a code-breaking quantum computer for years, and similar efforts by other well-funded security organizations may also be under way. In an alternative scenario, full-scale quantum computers arrive as commercial products and make encryption-cracking capabilities widely accessible.

Efforts to create quantum-resistant encryption are in progress. For example, the US National Institute for Standards and Technology (NIST; Gaithersburg, Maryland) is running a competition to encourage scientists to work on postquantum algorithms. However, new encryption standards will take time to develop. Dustin Moody, a mathematician at NIST's computer division, explains that "the whole process to study algorithms, standardise them and get them deployed…can take 15 years or longer" ("The quantum clock is ticking on encryption—and your data is under threat," *Wired*, 4 October 2016; online). Because quantum computers could arrive within 10 years, the 15-year timeline for the development of quantum-proof encryption is problematic.

Although quantum computing could create problems for current cryptography, principles of quantum mechanics are also beginning to enable new types of secure communication. Measuring a quantum system disrupts and changes that system. This fundamental principle of quantum mechanics makes quantum communications extremely difficult for a party to hack into without detection. Scientists are using quantum communications to transmit encryption keys securely over networks (networks sometimes need to transmit keys to set up encrypted communications, but such keys are vulnerable to theft). Quantum key distribution relies on quantum principles to enable two parties to create and share secret cryptographic keys. The two parties can then use these secret keys to encrypt and decrypt information for secure transmission over even insecure networks. Quantum key distribution already sees deployment on fiber-optic networks in the United States, Europe, and China, but current fiber technology supports quantum communications for distances of only as much as a few hundred kilometers. After that distance, the light signals become too faint. In August 2016, China launched the world's first quantum-communications satellite, which could eventually enable secure quantum communications over very long distances. Researchers aim to use the satellite to demonstrate quantum key distribution between stations more than 1,000 kilometers apart and to send impossible-to-crack keys from space to stations on the ground, thereby creating extremely secure quantum communications. Some researchers estimate that a functional network of quantum-communications satellites could become a reality in ten years. Governments, military organizations, and financial institutions will likely be the earliest users of space-based quantum communication because the technology necessary to enable it is so expensive; however, researchers are already looking for ways to make space-based quantum communication more widely accessible. For example, researchers from the Centre for Quantum Technologies (Singapore, Singapore) and the University of Strathclyde (Glasgow, Scotland) are developing low-cost CubeSats capable of delivering quantum key distribution.

SoC926

Signals of Change related to the topic:
SoC902 — Unusual Hacking…
SoC875 — Hacking to Manipulate
SoC870 — …Nanoscale Manufacturing…

Patterns related to the topic:
P0905 — Countering Surveillance
P0745 — Cyberattacks' New Dynamics
P0431 — Superfast Computing

STRATEGIC BUSINESS INSIGHTS

scan™

February 2017

P1022

Ubiquitous Cameras

By Marianne Monteforte (Send us feedback.)

Cameras are becoming ubiquitous and seeing use in a wide variety of applications.

Abstracts in this Pattern:
SC-2017-01-04-036 on Snap
SC-2017-01-04-051 on Citroën
SC-2017-01-04-095 on Sweden

Snap (Los Angeles, California), provider of image-messaging service Snapchat, plans to release Spectacles—sunglasses that use a built-in camera to take photos and record video. Spectacles will retail for $130 and be able to record as much as 30 seconds of video at a time. This product has sparked consumer concerns about privacy and surveillance—much as Google's (Alphabet; Mountain View, California) Google Glass smart glasses did a couple years ago. Nonetheless, consumer mind-sets are changing, and the success or failure of Spectacles will provide a good indication of whether the public is now prepared to tolerate such embedded cameras.

Social-media-based applications for cameras are extending their reach into the automotive industry. Automakers usually equip vehicles with dashboard cameras to serve as tools that monitor events such as accidents for insurance purposes or identify traffic situations for traffic-assistance features. But Citroën (Groupe PSA; Paris, France) is leveraging a camera behind the rearview mirror in the latest model of its C3 for a more frivolous reason: to enable drivers to take pictures and videos and post them on social-media platforms such as Snapchat and Instagram (Facebook; Menlo Park, California).

The emergence of new camera-based devices and applications often raises concerns about privacy and surveillance. For example, the Supreme Administrative Court of Sweden recently ruled that camera-equipped drones are surveillance cameras and banned anyone without a surveillance-camera permit from operating them. Acquiring such permits can be expensive, and paying the steep application fee does not guarantee that an applicant will receive a permit. In the future, similar rules could affect cameras on wearable-computing devices and other products.

Signals of Change related to the topic:
SoC897 — Live Streaming…
SoC804 — Cameras and Social Change
SoC511 — …More than Mementos

Patterns related to the topic:
P0766 — Cameras and Biometrics
P0340 — New Cameras, New Photography
P0155 — Advanced Camera Applications