Capítulo 13 (tradução Chat GPT -)
Conjeturas e Desafios da Gestão da Segurança. Um Olhar para o Futuro
Jean Pariès[1]

Resumo
As perturbações climáticas, mudanças demográficas, globalização, financeirização, fragmentação e complexificação industrial e econômica, digitalização em massa são todas mudanças significativas atualmente em curso no mundo e nas sociedades e, teoricamente, devem se acelerar até 2030–2040. O impacto dessas grandes tendências nas estratégias de gestão da segurança industrial é um tema pouco explorado, e é o foco deste livro colaborativo. Este capítulo final examina algumas das lições do livro e as coloca em perspectiva, oferecendo conjeturas sobre o papel do operador humano, a responsabilidade dos atores e das organizações, a confiabilidade e a vulnerabilidade dos sistemas sociotécnicos, a visão estratégica da segurança… Considerando esse leque de possibilidades e os desafios enfrentados pelo setor industrial, propõe caminhos a serem explorados para que, no futuro, os riscos continuem sendo gerenciados segundo os padrões esperados pela sociedade.

Palavras-chave
Confiabilidade humana · Responsabilidade · Estratégia de segurança · Antecipação · Complexidade · Instabilidade · Adaptação · Política

---

13.1 Mudanças no Mundo e Mudanças nas Mentes

Como muitos outros, este livro parte do pressuposto de que o mundo está passando por uma mudança global e radical, e, na escala da história das sociedades, isso está ocorrendo em um ritmo extremamente acelerado. De fato, tudo está mudando. O aquecimento global há muito anunciado confirma sua natureza inexorável e começa a mostrar seu poder de desestabilizar habitats, a economia, os modos de vida e as relações com o meio ambiente.

A população mundial continuará crescendo exponencialmente por décadas, especialmente na África, e estagnará e envelhecerá consideravelmente nas regiões economicamente mais desenvolvidas. Inevitavelmente, haverá uma redistribuição por meio de migrações em massa. A cadeia de produção de valor continua sendo transferida para países com mão de obra barata.

Suas organizações estão se tornando globalizadas, financeirizadas, fragmentadas e complexificadas em redes cada vez mais interdependentes. A digitalização galopante, a

H. Laroche et al. (eds.), *Managing Future Challenges for Safety*,
SpringerBriefs in Safety Management,
https://doi.org/10.1007/978-3-031-07805-7_13

virtualização, o aprendizado de máquina/profundo, junto com a conectividade em massa e o processamento de dados estão transformando as atitudes em relação à empresa, à produção e ao trabalho.

As apostas financeiras têm tamanha prioridade e são tão grandes que, no caso do 737 Max, a alta direção da Boeing impôs à sua lendária equipe de engenharia escolhas técnicas que desafiavam o bom senso e as regras básicas de projeto. As Big Five tornaram-se líderes da economia global. Seu valor de mercado ultrapassa em muito o PIB da França. O valor da Tesla alcançou a marca do trilhão de dólares, tornando-se cem vezes maior do que o da Renault e superior ao de todas as outras montadoras do mundo combinadas. Elon virou um nome popular.

A lista não termina aí, e o sentido mais profundo dessas transformações é objeto de debate. Mas, embora a trajetória ainda não esteja clara, uma coisa é certa: a escala e o ritmo das mudanças em curso são comparáveis aos das grandes "revoluções" da história. Em outras palavras, trata-se de uma metamorfose da sociedade. Com base nessa constatação, o livro levanta a questão: "Qual será o impacto dessa metamorfose nas estratégias de gestão de riscos industriais e, mais precisamente, no papel dos atores humanos nessas estratégias?" E, incidentalmente: "O que seria necessário fazer, hoje ou amanhã, para que, no futuro, o setor industrial continue gerindo seus riscos conforme os padrões esperados pela sociedade?"

Essas questões são difíceis por duas razões. Porque fazer previsões é uma arte difícil, especialmente em períodos de mudanças radicais. Mas também porque a própria noção de estratégia de segurança permanece pouco clara ou até contraditória em alguns aspectos. A introdução deste livro destacou isso ao colocar em perspectiva o modelo oficial de segurança, baseado na predefinição e no controle total, e um modelo prático que integra de forma mais realista as incertezas e as adaptações necessárias.

E o mundo "objetivo" não é o único que está mudando. Nossas representações mentais sobre ele também estão mudando, enquanto o mundo real permanece constante. Os modelos estão mudando; as próprias teorias estão passando por grandes "revoluções". E, nesse duplo processo, as mudanças da "realidade" e as mudanças da "teoria" interferem entre si. Como vimos com a COVID-19, certas certezas inabaláveis quanto à "ortodoxia orçamentária" ou aos benefícios da globalização foram… abaladas. O que era "impossível" tornou-se necessário. Inversamente, esse abalo na teoria também gerará ou facilitará mudanças na "realidade" econômica pós-COVID-19.

O mesmo ocorre no campo da segurança. Mais particularmente, no que diz respeito ao papel do operador humano na segurança, as visões e práticas industriais mudaram bastante nas últimas três décadas. A integração de conhecimentos das ciências humanas ao modelo de segurança o transformou profundamente. A visão do operador e da "confiabilidade humana" mudou. A equação inicial (segurança = confiabilidade técnica + operador obediente) tornou-se mais complexa. O operador passou a ser um

“agente de confiabilidade falível” em um ambiente reconhecido como menos previsível, exigindo adaptações em tempo real. E, assim, um operador “inteligentemente obediente” e líderes mais abertos, cooperativos e dispostos a escutar.

13.2 O Futuro da Injunction do “Operador Obediente e Inteligente”

Pode-se conjecturar que esse modelo será pouco afetado pelas transformações em curso. Já conhecemos a maioria dos processos em jogo: automação, virtualização das atividades por meio do distanciamento entre o operador humano e o processo físico em tempo real, substituição do operador por robôs, transformação do ator em supervisor. Essas mudanças já ocorreram em várias indústrias, especialmente na aviação. Elas se espalharão para outras indústrias e, dentro de cada uma, para ocupações mais “altas” na hierarquia (por exemplo, médicos em vez de enfermeiros). Isso mobilizará novas tecnologias mais disruptivas e envolverá interações homem–máquina complexificadas pela inteligência artificial (IA) e pelo aprendizado de máquina.

No geral, os operadores remanescentes terão ainda mais dificuldade para construir um “modelo mental” da máquina e para prever e compreender o que ela está fazendo. Já conhecemos os efeitos negativos associados: excesso de confiança na máquina; perda de compreensão; problemas de vigilância; perda de saberes básicos, que permanecem cruciais em modo degradado. Também sabemos que eles podem ser parcialmente controlados e que o resultado final é, na maioria das vezes, favorável ou até altamente favorável à segurança.

A conjectura mais razoável, portanto, é que o número de problemas de segurança associados à confiabilidade dos operadores da linha de frente continuará a cair significativamente no que se refere ao funcionamento projetado e normal. Um corolário é que a responsabilidade deve passar dos usuários dos sistemas para seus projetistas — a menos que, como a Tesla e seus colegas, esses projetistas consigam convencer a todos de que os operadores estão sempre “no controle” dos referidos sistemas.

No entanto, a capacidade dos operadores de intervir e retomar o controle em situações “além do escopo de projeto” também diminuirá drasticamente. E será cada vez menos possível que os operadores compensem essa tendência com um melhor conhecimento dos sistemas que operam, pois estes terão se tornado complexos demais e inevitavelmente “esotéricos” em modo degradado.

Caso ainda sintamos a necessidade de manter algum nível de controle sobre situações “além do escopo de projeto”, a capacidade de interpretação da equipe operacional terá de ser aprimorada oferecendo acesso em tempo real à rede de especialização

necessária, e os sistemas precisarão ser projetados para incluir um modo de operação que não exija acesso à causalidade — semelhante ao "controle baseado em estados" utilizado em usinas nucleares quando a compreensão adequada se perde, em contraste com o controle baseado em eventos. Isso implicará treinar os projetistas em complexidade, suas consequências e sua gestão — muito mais do que se faz atualmente.

Mas, no nível da organização, da empresa e ainda mais no nível da sociedade como um todo (público, mídia, justiça, arena política), a estratégia de segurança ainda é amplamente percebida como resultante da capacidade de antecipar todas as situações, de predeterminar as soluções técnicas e humanas adequadas e de assegurar conformidade com o que foi antecipado. Tudo isso por meio de uma formalização cada vez mais detalhada, uma "racionalização" do sistema, dos processos e das atividades, e por meio da garantia de sua qualidade ("escrevemos o que fazemos, fazemos o que está escrito, e é isso que nos protege contra processos judiciais caso ocorra um acidente"). Em resumo, um modelo de máquina programada, determinista e linear, controlada por um sistema de "comando e controle" todo-poderoso, que nada sabe sobre situações "além do escopo de projeto".

13.3 Ascensão e Queda de uma Mudança de Paradigma

No entanto, ao menos nas últimas três décadas, algumas correntes científicas[1]([2]) vêm propondo outras visões de segurança, baseadas no reconhecimento da complexidade dinâmica dos sistemas sociotécnicos que constituem o mundo industrial. Essa "complexidade" implica variabilidade constante e irredutível, turbulência, causalidade circular, não linearidade entre causas e efeitos, interferência, ressonância, acoplamentos de longo alcance, "efeito borboleta" etc. Nesse mundo, a variação faz parte do estado normal e é o ruído de fundo irredutível da "vida" do sistema. A metáfora subjacente já não é a de uma máquina programada, mas sim a de um sistema vivo. Sua sobrevivência não implica a ausência de desvios (pelo contrário, estes são parte integrante da sua evolução), mas sim o gerenciamento constante desses desvios, bloqueando os desfavoráveis e selecionando os favoráveis à adaptação e à adaptabilidade. E, nessa visão, a segurança é inseparável dos demais objetivos vitais: não é possível obter comida ou água sem se expor a predadores. A resiliência só pode ser pensada como compromisso entre diferentes necessidades de sobrevivência.

Diferentemente da abordagem de fatores humanos e organizacionais (HOF), essa visão sistêmica não foi "adotada" pela segurança industrial. Pelo menos, não em sua totalidade. É possível identificar certos aspectos que foram parcialmente apropriados. A crise da COVID-19 banalizou o termo "resiliência" e aguçou nossa consciência de que

[2] E.g., Normal Accident Theory (C. Perrow); High Reliability Organizations (T. Laporte & al.); Risk Management in a Dynamic Society (J. Rasmussen); Systems Theoretic Hazard Analysis Technique (N. Leveson); Resilience Engineering (D. Woods, E. Hollnagel & al.).

a única certeza é a incerteza — ou seja, que coisas inesperadas e imprevisíveis acontecerão. Mas, como já mencionado, o "paradigma" da segurança continua essencialmente atrelado à antecipação e à predefinição. Pode-se até dizer que está se fortalecendo, com o aumento de normas e dos esforços de conformidade. Aliás, estes são amplamente validados pelos avanços inegáveis — e, por vezes, consideráveis — alcançados na segurança nas últimas décadas. E hoje, a maioria dos projetistas e estrategistas do setor industrial aguarda um novo avanço nessa estratégia, graças aos progressos espetaculares na digitalização, IA, big data, gêmeos digitais e aprendizado profundo, que acreditam trazer um salto nas capacidades de modelagem, previsão e monitoramento.

Entretanto, as análises relatadas neste livro indicam claramente que a atual revolução sociotecnológica gerará tensões intensas, típicas de grandes transformações sociais e dos desafios de adaptabilidade que elas acarretam. A Europa provavelmente enfrentará uma forte escassez de competências especializadas devido ao descompasso entre a formação oferecida por suas universidades e as necessidades de seu setor industrial. O envelhecimento de sua força de trabalho entrará em conflito com a necessidade de ter várias ocupações ao longo da carreira. Sua conversão cultural, cada vez mais favorável ao respeito ao meio ambiente e a uma vida mais frugal ou até ascética, dificilmente será seguida pelo restante do mundo — ao menos num primeiro momento. Corre-se o risco de uma transferência consecutiva dos centros nervosos de suas indústrias — projeto, normalização, financiamento — para a Ásia, prolongando a migração das cadeias de produção de valor.

Com a fragmentação e globalização do setor industrial, as inovações tecnológicas em curso — e as que ainda virão — superarão a capacidade de monitoramento e certificação dos órgãos reguladores para garantir a segurança, como já ilustrado pelos desafios da certificação de sistemas que aprendem sozinhos. A lacuna aumentará entre aqueles (projetistas, grandes players) que compreenderão os algoritmos e terão acesso aos dados e aqueles que apenas os "consumirão" sem entender. A autorregulação e os terceiros (seguradoras, organismos de normalização, alianças profissionais) substituirão cada vez mais as autoridades oficiais. Falhas sistêmicas em redes computacionais e a cibersegurança substituirão a confiabilidade do operador como principal preocupação em relação à "segurança". Com a perda de inteligibilidade e a crescente dissociação entre benefício e risco, a aversão ao risco por parte do público, usuários e moradores locais continuará a crescer — e, com ela, a desconfiança e a suspeita, amplificadas pelas redes sociais, em um mundo cada vez mais esotérico ou até mágico, mergulhado em um modo de "emergência", desestabilizado pelas mudanças climáticas e pelos efeitos bumerangue da destruição dos ecossistemas. Cada vez mais riscos se tornarão inasseguráveis.

Além dessa previsão — que inevitavelmente estará errada e que, espera-se, representa uma visão pessimista —, a revolução sociotecnológica em curso pode, portanto, gerar um verdadeiro paradoxo. Ao estender o tecido industrial a uma escala global enquanto o fragmenta e multiplica as interconexões, a revolução aumenta inexoravelmente sua complexidade e, portanto, por definição, os limites à sua modelagem, bem como a incerteza e o potencial de "surpresas fundamentais" a ela associadas. Ao mesmo tempo, cresce a sensação de que o poder computacional está se desenvolvendo mais rápido do que o objeto da modelagem: já que um futuro totalmente pré-calculável está agora ao alcance com os gêmeos digitais, a predefinição exaustiva e o controle total estariam logo ali. E poderia haver, enfim, um "fim da gestão de riscos de segurança".

Nisso, há, sem dúvida, uma ilusão do mesmo tipo da que, no final do século passado, acreditava na chegada do "fim da história". Isso não significa que todas as promessas da tecnologia digital sejam falsas. É certo que teremos fábricas, trens, aviões e reatores nucleares controlados em níveis uma ordem de grandeza superiores aos nossos melhores níveis atuais. Mas — e isso é uma obviedade — esse controle jamais será total. E, mais importante, dirá respeito a processos locais, e não ao sistema como um todo. Os acidentes se tornarão mais raros, mas cada vez mais do tipo "cisne negro".

Comentado [IMA1]: 1.O conceito do Cisne Negro (black swan) se refere a **eventos financeiros difíceis de prever** (outliers ou "pontos fora da curva"). Foi criado pelo filósofo Nassim Taleb e diz respeito a eventos que impactam com tanta força o mercado, que as pessoas são obrigadas a olhar em retrospecto.

2. Wikipédia:
A **Teoria do Cisne Preto** foi concebida por Nassim Nicholas Taleb.[1] Ela é utilizada para explicar:
2.1. Um acontecimento de impacto desproporcionado ou um evento raro aparentemente inverosímil, para lá das expectativas normais históricas, científicas, financeiras ou tecnológicas.
2.2 A impossibilidade de calcular a probabilidade de eventos raros, porém consequentes, através de métodos científicos (dada a ínfima probabilidade da sua natureza).
2.3 O viés psicológico que leva uma pessoa individualmente ou coletivamente a não ver ou não querer ver a importância decisiva de determinado evento raro no desenrolar da História.

13.4 O Risco de uma Evolução Tardia e Estéril da Gestão da Segurança

Assim, tudo se passa como se a história da segurança fosse a de uma lenta ascensão pelos níveis da organização: começando com a máquina, o operador e seu posto de trabalho, passando pelo nível das equipes, oficinas, procedimentos, depois os processos, os departamentos, os locais de produção. Mas também tudo se passa como se a estratégia de segurança estivesse sempre um nível atrasada. Quanto mais complexo o sistema se torna, mais os fatores de raiz — que "produzem" o risco e permitem sua modulação — se deslocam para o nível superior seguinte. Pensamos no nível do posto de trabalho quando já são o projeto e os processos que estão em causa, pensamos no nível do processo quando o problema já está na estratégia da empresa, e pensamos no nível estratégico da tomada de decisão quando, na verdade, é a cadeia global de produção de valor que está gerando instabilidades… E embora os estudos de segurança sejam realizados para mudanças internas e locais dentro da empresa, isso não ocorre para as grandes mudanças que afetam o mundo. A segurança está saindo dos limites da empresa, e sua dimensão sistêmica não está sendo tratada no nível apropriado. Se não tomarmos cuidado, o futuro da segurança se parecerá com o dos antibióticos: dada nossa estratégia de esterilização, a ameaça do futuro não é tanto o patógeno original, mas o fato de que nossas defesas estarão sempre uma mutação atrasadas.

Portanto, é importante sair dos círculos voltados para a segurança para falar sobre segurança. Os desafios à segurança estão em outro lugar, em espaços pouco

penetrados pela segurança. Uma das constatações da "Análise Estratégica²"[3] que fundamenta este livro é que as grandes mudanças no mundo estão sendo questionadas por pesquisadores e especialistas de diversas áreas, examinadas sob inúmeros ângulos, mas não sob o ângulo da segurança — ou, pelo menos, não como prioridade. A segurança aparece como uma dimensão órfã da reflexão. Os grandes desafios climáticos, ambientais, econômicos e geopolíticos também são discutidos em círculos influentes, em think tanks que reúnem líderes mundiais, nas COPs, em Davos e similares. Por outro lado, embora a segurança sistêmica hoje ultrapasse os lugares tradicionais de discussão — que são a empresa e sua relação com os órgãos reguladores —, há poucos, se é que há, espaços onde ela é debatida. São raras as publicações, encontros, organizações que discutem o impacto das grandes mudanças na segurança.

Nas empresas, os responsáveis continuam pensando a segurança industrial associada ao "estado interno" da organização, mesmo que suas fronteiras já tenham se dissolvido. Assim, como as grandes mudanças se dão em círculos onde a segurança não é tema de discussão, o desafio é levantar as questões de segurança nesses espaços de influência, criar novos espaços de influência onde elas possam ser tratadas e reforçar os poucos que já existem. Isso não será fácil. Os temas são ditados pela escala e urgência dos problemas. Diz-se que Stalin respondeu a Pierre Laval, então primeiro-ministro francês em visita a Moscou, que lhe pediu um gesto favorável ao Vaticano: "O Papa? Quantas divisões ele tem?" Nossos estrategistas perguntarão: "Segurança? Quantos bilhões?" Comparada às consequências de pandemias, aquecimento global, aumento de eventos climáticos extremos e ataques cibernéticos, será pouco. E, com o foco crescente em alguns raros cisnes negros, pode parecer ainda menos audível pelo megafone das redes sociais. Os especialistas em segurança terão de aprender seriamente as lições da influência de massa e do lobby. Em outras palavras, da política.

---

[3] Research methodology developed by FonCSI that brings together international academics and practitioners for inquiry and debate, and aims at providing FonCSI's partners with high-level results within 18–24 months.