今世紀の初め、セキュリティ技術は相互に疑わしい島々の群島でした。暗号学者、オペレーティングシステム保護担当者、盗難警報器業界、そして紙幣のインクを作った化学者に至るまでです。  
2010年までに、セキュリティエンジニアリングは確立された成長する分野でした。開業医が私たちが快適ゾーンを超えて見なければならないことに気づいたので、島々は橋によってつながれていました。  
現在、2020年には、実際の製品やサービスに効果的に統合できるコンポーネントを設計するために、誰もがシステムの視点を持つ必要があります。  
セキュリティエンジニアリングとは、爆撃機からボットネットまで、あらゆる種類の悪意に直面しても、システムが予測可能に信頼できるようにすることです。  
したがって、スタッフ（顧客、ユーザー、傍観者）の現実的な理解が不可欠です。人的、組織的、経済的要因は、技術的要因と同様に重要です。  
目標間の対立は一般的です。あるプリンシパルが説明責任を望み、別のプリンシパルが否認を望んでいる場合、両方を満足させることは困難です。  
これは安全経済学の成長につながりました、それはこの本の最初の版が触媒するのを助けました。  
それでは次は？  
まず、複雑さ。  
高速道路や砂漠でかなりうまく運転できるように車をプログラムすることはできますが、予測できない人々がいる雑然とした街の通りには対処できません。  
そして、いじめには限界があります。 「コンピュータはノーと言う」は顧客を失う速い方法です。  
第二に、持続可能性。  
車、ペースメーカー、変電所などの耐久性のある商品では、ソフトウェアを20年または40年も維持しなければならない場合があります。  
いわゆる「スマート」デバイスは、多くの場合、「コンピュータがノーと言った」ときに、すぐに捨てなければならないものです。  
セキュリティはスカラーではなく、関係です。  
「コンピューターがノーと言う」ときに誰が負け、誰が利益を得るのか  
 お金を政治権力に変えるためにどのように使用されますか？  
 テクノロジーが完全に変化した10年以上にわたるサイバー犯罪の安定性は、それがテクノロジーに関する根本的な問題ではないことを示唆しています。  
Facebookが政治演説の仲裁者になったとき、AppleとGoogleがコロナウイルスの連絡先追跡に関するポリシーを指示できるとき、およびAmazon、Microsoft、Googleが顔認識に関するポリシーを指示したとき（中国以外）  
今後10年間で最も扱いにくい問題は、ガバナンスに関係する可能性があります。  
民主主義はそのための重要なメカニズムです。  
テクノロジーが複雑さ、持続可能性、権力の性質について提起する問題に取り組むほど、私たちの社会はより速くそれらに対処するようになります。