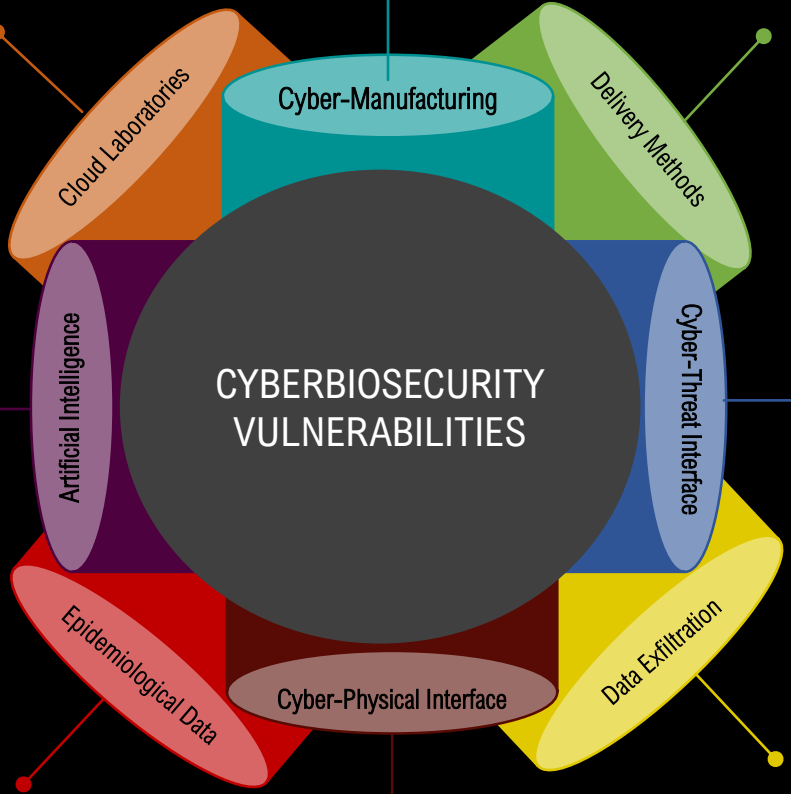
CYBER-AI-BIO CONVERGENCE

Eleonore Pauwels,
Director, Anticipatory Intelligence Lab
Woodrow Wilson International Center for Scholars



BIO-INDUSTRY

008
AI-Data Manipulation

Cloud-based bench technologies present tempting targets for data theft

007
AI Adversarial Attacks

Artificial intelligence is not fully shielded and thus may be influenced with malicious intent

PRECISION AGRICULTURE

006
Pathogen Tracking

Public health, wildlife, and agricultural records reveal important patterns in vector distribution

INFECTIOUS DISEASES

001
Automated Lab Hacking

Cloud-based security cannot fully shield important genomic foundry and engineering data

005
Digital Medicine

Digital assistive technologies (artificial organs, etc.) can be compromised and mined

PRECISION MEDICINE

002
Genetic Treatments

Personalized and unique genomic treatments are developed from cloud-based patient data

003
Patient Portals

Patients rely increasingly on medical management software, creating additional security risks

004
Data Exfiltration

Data used to create drugs, weapons, and other research can be mined, hacked, or manipulated

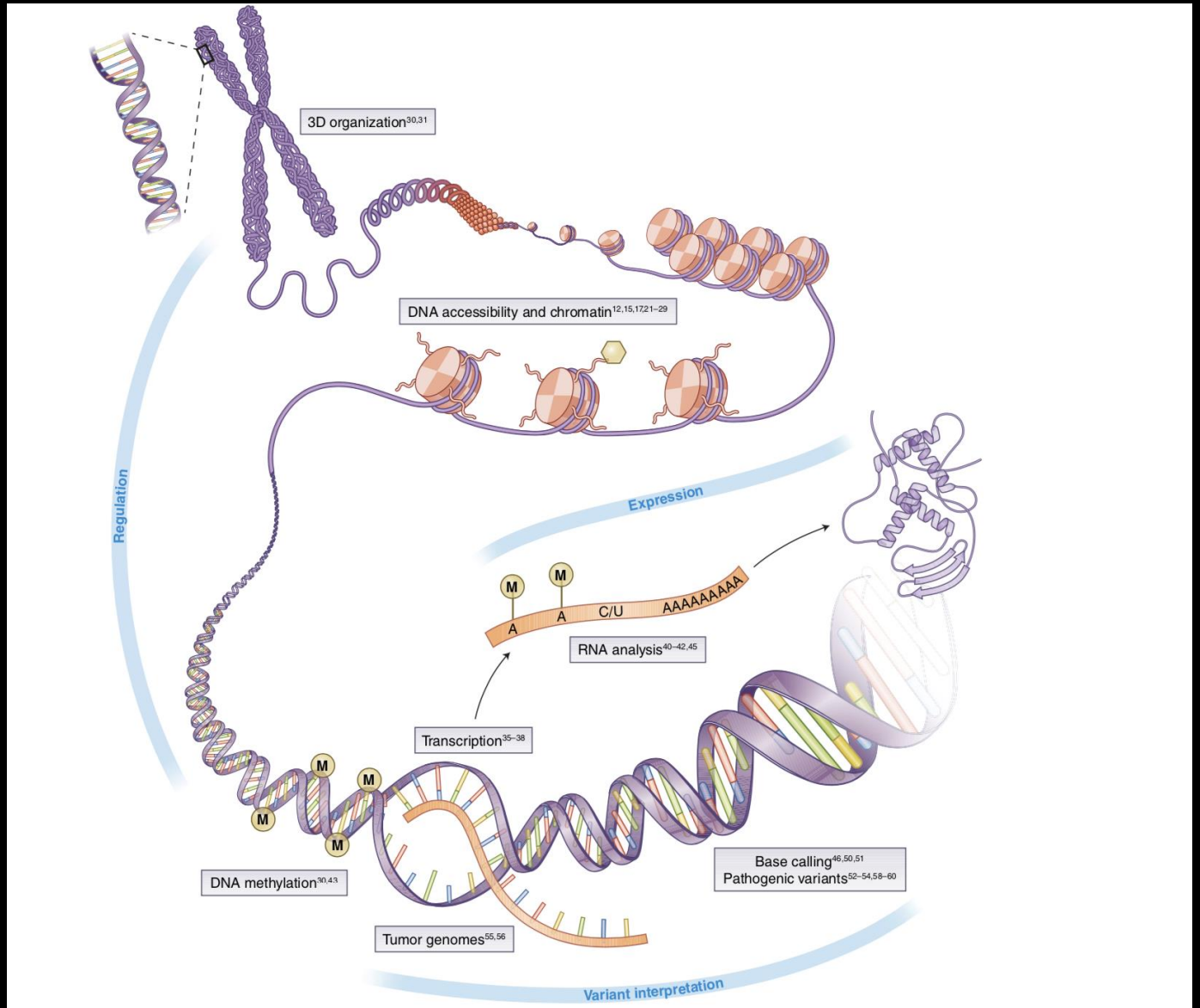
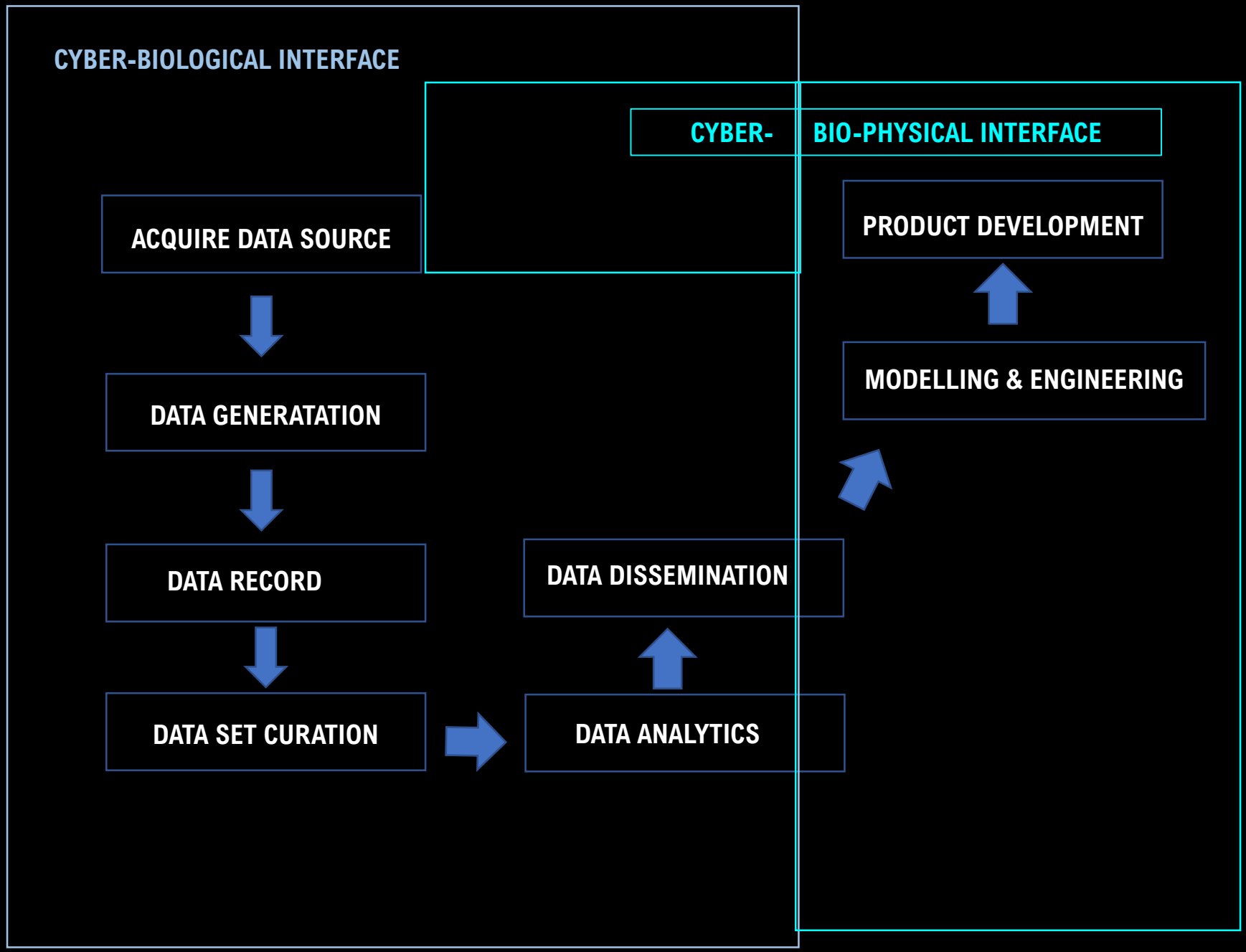


Fig. 2 | Applications of deep learning in genomics. The boxes highlight several application domains and references discussed in the text. Image adapted with permission from ref. [65], Springer Nature.

Source: Figure 2 from Zou, et al. 2019. "A Primer on deep learning in genomics." *Nature Genetics Perspective*; Vol. 51, January. (p. 15)

AUTOMATED BIO-LABS / CLOUD LABS / BIO-FOUNDRIES


CYBER-BIOLOGICAL INTERFACE
CYBER-
BIO-PHYSICAL INTERFACE
ACQUIRE DATA SOURCE
DATA GENERATATION
DATA RECORD
DATA SET CURATION
DATA ANALYTICS
DATA DISSEMINATION
PRODUCT DEVELOPMENT
MODELLING & ENGINEERING

CYBER-BIOSECURITY RISKS

BIOSECURITY RISKS
Obtaining genomic data to do harm
Using genomic data to engineer new pathogens
Using genomic data to recreate extinct, high-impact pathogens
Using genomic data to modify low-risk pathogens to become high-impact
Using genomic data to increase the likelihood of disease
Using genomic data to enhance targeting of the recipient
Using genomic data to enhance pathogens
CYBERSECURITY RISKS
Waging adversarial attacks on automated bio-computing systems, biotech supply chains, or strategic cyber-biosecurity infrastructure
Manipulating and/or editing data deliberately to be incorrect
Accessing proprietary or high-risk information without authorization
Stealing proprietary or high-risk data
Stealing proprietary tools to analyze datasets
Transferring data securely to the correct end users

ADVERSARIAL ATTACK ON MEDICAL AI